

Analysis of Perception and Readiness for Preemptive Cybersecurity Implementation as a Cyber Threat Prevention Strategy

Trija Anjelia^{1*}, Mambang^{2*}, Jibrillian Gilang Satriaji^{3*}, Mahdi^{4*}, Ahmad Riqi Ramadhani Cahyono^{5*}

^{*} Information Technology, Faculty of Science and Technology, Sari Mulia University, Banjarmasin
trija.anjelia@student.unism.ac.id¹, mambang@unism.ac.id², jibrillian.gs@student.unism.ac.id³,
mahdi.unism@student.unism.ac.id⁴, riqi.ramadhani@student.unism.ac.id⁵

Article Info

Article history:

Received 2026-06-14

Revised 2026-09-11

Accepted 2026-10-14

Keyword:

*Artificial Intelligence,
Cyber Threat Intelligence,
Preemptive Cybersecurity,
Threat Hunting,
Cybersecurity Readiness*

ABSTRACT

The increasing complexity of cyber threats requires organizations and individuals to adopt proactive cybersecurity strategies. This study aims to analyze perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. A quantitative approach was employed using a cross-sectional survey distributed through Google Forms. A total of 45 valid responses were collected and analyzed using descriptive statistical analysis. The study examined five dimensions, namely Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), Vulnerability Assessment (VA), and Readiness (RD). The findings indicate that respondents generally have positive perceptions toward proactive cybersecurity practices and demonstrate a high level of readiness to support preventive cybersecurity initiatives. The readiness dimension achieved the highest mean score, highlighting the importance of anomaly reporting, organizational transparency, and continuously updated security systems. Overall, the results suggest that Preemptive Cybersecurity is positively perceived as an effective approach for improving cyber resilience and preventing cyber threats.



This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

I. INTRODUCTION

Developments in digital transformation have driven the widespread use of information technology in various fields, including government, education, healthcare, and industry [1]. The application of technologies such as cloud computing, Internet of Things, artificial intelligence, and internet-based digital services has improved operational efficiency and accelerated information exchange [1],[2]. However, the increased reliance on digital technology also expands the areas that cybercriminals can attack [2],[3]. Various types of cyber threats such as ransomware, phishing, malware, and Advanced Persistent Threats (APT) continue to evolve with increasing levels of complexity, posing risks to the confidentiality, integrity, and availability of information [3],[4],[5]. This situation shows that organizations need a more proactive and adaptive cybersecurity strategy to deal with changing threats and maintain operational continuity in the digital era [5],[6].

Reactive cybersecurity approaches are still widely adopted by many organizations to protect their digital assets and information systems. This method emphasizes identification, response, and recovery after a security incident occurs, so it is often not effective enough in avoiding the effects of an attack in the first place [7]. In addition, the reliance on signature-based detection mechanisms causes reactive systems to have limitations in identifying new threats including zero-day exploits and malware that continue to evolve to evade detection [7],[8]. The development of increasingly complex cyber threats, accompanied by the use of artificial intelligence (AI) by attackers, poses new challenges for organizations in maintaining information system security. In addition, the need to analyze large amounts of security data in real-time makes security approaches that focus on response after an incident occurs are less effective in dealing with modern threats [9]. Therefore, organizations need to implement a more proactive and adaptive security strategy

so that potential threats can be identified and minimized before they cause disruptions to operations and information security [9].

As digitalization increases and the use of interconnected technologies, such as the Internet of Things (IoT), cloud computing, and data-driven automation, organizations face increasingly complex security challenges. Traditional security approaches that are reactive and rely on signature-based detection mechanisms are considered inadequate in the face of modern cyber threats that are constantly evolving [10]. Alternatively, Preemptive Cybersecurity emerges as an approach that leverages predictive analytics and Machine Learning (ML) to identify potential threats based on historical data patterns and emerging risk indicators [10],[11]. Through the use of structured and unstructured data and continuous analytical capabilities, this approach enables organizations to anticipate threats early, strengthen cyber resilience, and reduce the likelihood of exploitation before a successful attack is carried out [11],[12].

In the cybersecurity literature, several related but distinct concepts are frequently used. Proactive cybersecurity generally refers to any defensive posture that seeks to act before an incident occurs, encompassing practices such as continuous monitoring, threat hunting, and vulnerability management [10],[11]. Predictive security focuses more narrowly on forecasting future threats through statistical modeling, machine learning, and risk scoring based on historical and real-time data [11],[12]. Cyber threat prevention is a broader goal-oriented term describing the overall objective of stopping attacks before impact. In this study, Preemptive Cybersecurity is defined as a specific strategic orientation that integrates predictive analytics, continuous threat anticipation, active hunting of latent threats, and early mitigation actions with the explicit aim of neutralizing threats before they materialize into security incidents. It is therefore positioned as a more action-oriented and integrated subset of proactive cybersecurity that combines predictive capabilities with deliberate preemptive intervention [10],[11].

Cyber Threat Intelligence (CTI) is evidence-based knowledge that includes information about the characteristics, indicators, and mechanisms of cyber threats that can be used to support security decision-making [13]. In the implementation of Preemptive Cybersecurity, CTI plays an important role in helping organizations identify potential threats, vulnerabilities, and security risks before they develop into a cyber incident with significant impact [14]. In addition, CTI allows organizations to understand the Tactics, Techniques, and Procedures (TTPs) used by threat actors, so that defense strategies can be developed more effectively and sustainably [12],[15]. By providing relevant and actionable information, CTI supports faster, more accurate, and data-driven decision-making processes in an effort to protect the organization's critical assets and infrastructure [14],[15].

Threat Hunting is a proactive approach that aims to identify undetected threats or suspicious activities that have the

potential to harm an organization's systems [16]. In contrast to traditional monitoring mechanisms that generally rely on signatures or specific detection rules, Threat Hunting involves active investigation of anomalies, indicators of compromise (IoCs), and patterns of behavior that may indicate the presence of cyber threats [16]. The implementation of Threat Hunting is closely related to Cyber Threat Intelligence (CTI), because information about Tactics, Techniques, and Procedures (TTPs) obtained from CTI can be used as a basis for identifying and prioritizing potential threats that need to be explored further [17]. Through the combination of CTI and Threat Hunting, organizations can improve their early detection capabilities, reduce the risk of hidden threats, and strengthen Preemptive Cybersecurity strategies in the face of an ever-evolving threat landscape [13], [17].

The development of Artificial Intelligence (AI) makes a significant contribution in supporting the implementation of Preemptive Cybersecurity [18]. AI's ability to analyze large amounts of security data allows organizations to identify threat patterns, anomalies, and attack indicators that are difficult to detect through conventional methods [18],[19]. In addition to supporting the threat analysis process, AI also plays a role in strengthening Cyber Threat Intelligence (CTI) and Threat Hunting through automation of data processing, identification of attack patterns, and faster and adaptive decision-making [19],[8]. Therefore, the use of AI is one of the important factors in realizing a more predictive, proactive, and prevention-oriented security strategy [8].

Vulnerability Assessment (VA) is the process of identifying, analyzing, and evaluating weaknesses in information technology systems, networks, applications, and infrastructure that have the potential to be exploited by attackers [20]. In the context of Preemptive Cybersecurity, the VA plays an important role in helping organizations recognize security risks and vulnerabilities that can threaten operational continuity before they are exploited by threat actors[20],[21]. Through regular security scans, configurations, and evaluations, organizations can prioritize mitigation and strengthen the security controls that have been implemented [21]. In addition, the implementation of a continuous risk assessment approach and the use of automation technology allows vulnerability identification to be carried out more quickly and accurately, supporting a more proactive, adaptive, and prevention-oriented security strategy [21],[22].

Although various studies have discussed the application of cybersecurity technology to reduce the risk of digital threats, the success of cybersecurity implementation does not only depend on technical aspects, but is also influenced by the readiness of the organization as a whole [23]. This readiness includes security governance, management support, security culture, and human resource competence in dealing with evolving cyber threats [23],[24]. In addition, an organization's ability to adopt and utilize security technology effectively is an important factor in building sustainable

cyber resilience [24]. Therefore, organizational readiness is one of the main aspects that need to be considered in the implementation of a proactive and adaptive cybersecurity strategy [25].

The selection of the five dimensions examined in this study Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), Vulnerability Assessment (VA), and Readiness (RD)—is grounded in the complementary roles these components play within a preemptive defense model. CTI provides the knowledge foundation (indicators, TTPs, and threat context) that informs subsequent actions [13],[14],[15]. Threat Hunting operationalizes this knowledge through active, hypothesis-driven investigation of latent threats [16],[17]. AI supplies analytical scale and speed, enabling pattern recognition and automation that amplify both CTI processing and hunting effectiveness [8],[18],[19]. Vulnerability Assessment closes the loop by continuously identifying and prioritizing exploitable weaknesses before adversaries can leverage them [20],[21],[22]. Readiness functions as the enabling organizational condition—encompassing policy orientation toward prevention, reporting culture, investment priorities, system currency, and transparency—without which technical capabilities cannot be sustained [23],[24],[25]. Conceptually, CTI, TH, AI, and VA represent the core operational and technological pillars of Preemptive Cybersecurity, while RD represents the human and organizational capacity required for their adoption and effective use.

The rapid digital transformation in Indonesia, characterized by the increasing adoption of information technology, has led to the emergence of increasingly complex cyber risks and threats [26]. This condition highlights various challenges in cybersecurity preparedness, including limited cybersecurity awareness, inadequate technical competencies, and the need for stronger security practices among digital technology users [27],[28]. At the same time, the transition from reactive cybersecurity approaches to more proactive and preventive strategies has become increasingly important in addressing evolving cyber threats [27]. However, empirical studies that specifically examine public perceptions and readiness regarding the implementation of Preemptive Cybersecurity remain limited, particularly in developing countries and emerging digital environments, particularly in understanding how individuals perceive the benefits, challenges, and strategic importance of proactive cybersecurity approaches [28]. Therefore, this study was conducted to provide an overview of public perceptions and readiness toward the implementation of Preemptive Cybersecurity as a more effective and adaptive cyber threat prevention strategy.

While prior research has examined cybersecurity awareness, general proactive practices, or organizational readiness in isolation [23],[24],[25],[28], this study contributes by focusing specifically on Preemptive Cybersecurity as an integrated conceptual construct and by jointly assessing percep-

tions of its key operational dimensions (Cyber Threat Intelligence, Threat Hunting, Artificial Intelligence, and Vulnerability Assessment) together with readiness to support their implementation. The novelty lies in clarifying the conceptual boundaries of Preemptive Cybersecurity relative to related terms, providing an exploratory empirical snapshot of how these dimensions are perceived among digitally active individuals in an Indonesian higher-education and technology-user context, and highlighting readiness indicators that organizations may prioritize when advancing prevention-oriented strategies. The study remains primarily descriptive and exploratory; it does not claim to establish causal effectiveness of Preemptive Cybersecurity in improving cyber resilience.

Based on the foregoing discussion, this study aims to analyze public perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. In addition, this study describes respondents' perceptions regarding Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), and Vulnerability Assessment (VA) as key components supporting proactive cybersecurity practices. The findings are expected to provide empirical insights into the level of readiness and acceptance of preventive cybersecurity approaches, as well as contribute to the development of more adaptive and sustainable cybersecurity strategies.

II. METHOD

This study employed a quantitative survey-based approach to analyze respondents' perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. Quantitative research is widely used to collect and analyze numerical data through structured questionnaires, enabling researchers to identify patterns, describe attitudes, and evaluate readiness levels toward a particular phenomenon [29],[25]. The research process consisted of questionnaire distribution, data collection, Exploratory Data Analysis (EDA), and descriptive statistical analysis to provide a comprehensive understanding of respondents' perceptions and readiness regarding proactive cybersecurity practices[30].

A. Research Design

This study employed a quantitative research approach to examine perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. Quantitative research systematically investigates phenomena using numerical data and statistical analysis and is commonly conducted through survey-based data collection methods [29]. This study employed a quantitative research design using a cross-sectional survey approach to analyze public perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. A cross-sectional design was selected because the data were collected from respondents at a single

point in time, allowing the researcher to capture current perceptions and readiness levels regarding proactive cybersecurity practices. Survey-based research is widely used to measure attitudes, beliefs, and perceptions of respondents through standardized questionnaires, enabling the collection of numerical data that can be analyzed statistically.

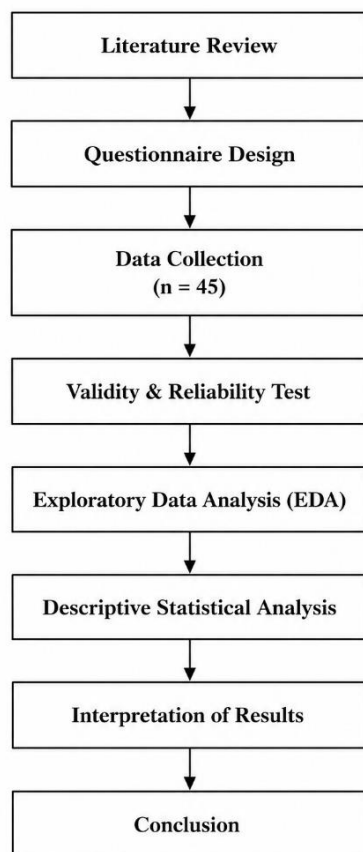


Figure 1. Research Process Flow

B. Research Framework

Preemptive Cybersecurity emphasizes proactive measures to identify, anticipate, and mitigate cyber threats before they develop into security incidents. Based on the literature review, Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), and Vulnerability Assessment (VA) are recognized as key components that support the implementation of proactive cybersecurity strategies. These components enable early threat detection, enhance situational awareness, improve decision-making processes, and strengthen preventive security controls.

In this study, Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), Vulnerability Assessment (VA), and Readiness (RD) were examined as key dimensions of Preemptive Cybersecurity. Readiness reflects the extent to which individuals are prepared to adopt proactive cybersecurity practices and support preventive approaches to cyber threat mitigation. The research framework

was developed to illustrate these dimensions and provide a conceptual overview of respondents' perceptions and readiness toward the implementation of Preemptive Cybersecurity.

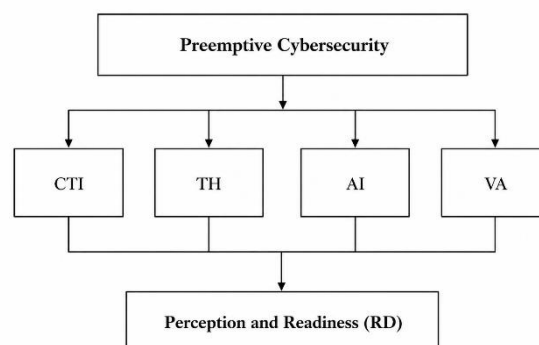


Figure 2. Research Framework

Figure presents the conceptual framework of this study. The framework describes the main dimensions associated with Preemptive Cybersecurity implementation and respondents' readiness toward proactive cybersecurity practices.

C. Population and Sample

The target population of this study consisted of individuals who actively use digital technologies and internet-based services. Since the study aims to investigate perceptions and readiness toward the implementation of Preemptive Cybersecurity, respondents were selected based on their familiarity with information technology and cybersecurity-related issues.

A purposive sampling technique was employed to ensure that the selected respondents possessed sufficient experience and understanding of digital technology usage. Data collection was conducted through an online questionnaire distributed via Google Forms. A total of 45 valid responses were obtained and included in the final analysis. The study was intended as an exploratory assessment of perceptions and readiness toward Preemptive Cybersecurity. Therefore, the sample size was considered sufficient to provide initial insights into respondents' views regarding proactive cybersecurity practices.

The selected respondents represent users who regularly interact with digital systems and online platforms, making them relevant participants for assessing perceptions and readiness regarding proactive cybersecurity practices.

D. Research Instrument

The research instrument used in this study was a structured questionnaire distributed online through Google Forms. The questionnaire consisted of two sections. The first section collected respondents' demographic information, including age, gender, educational background, occupation, and frequency of experiencing cyber threats. The second section contained statements designed to measure the research constructs related to Preemptive Cybersecurity.

The questionnaire items were developed based on the key components of Preemptive Cybersecurity identified in the literature review, namely Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), Vulnerability Assessment (VA), and Readiness for Preemptive Cybersecurity Implementation. A total of 20 measurement items were used to assess these constructs.

Responses were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The Likert scale was selected because it enables respondents to express their level of agreement toward statements related to cybersecurity perceptions and readiness. Higher scores indicate stronger agreement with the implementation of proactive cybersecurity practices.

TABLE I
RESEARCH VARIABLES AND INDICATORS

Variable	Code	Indicator
Cyber Threat Intelligence (CTI)	CTI1	The organization/system has tools capable of detecting suspicious activities before cyberattacks occur.
	CTI2	Information regarding external security threats helps in developing better protection and defense strategies.
	CTI3	Monitoring suspicious activities in less accessible parts of the internet helps prevent future security threats.
	CTI4	The system is capable of identifying attacker tactics and attack patterns before they infiltrate the network.
Threat Hunting (TH)	TH1	Security strategies focus on actively searching for potential threats rather than waiting for alerts or incidents.
	TH2	The use of deception-based security mechanisms can help protect critical data assets.
	TH3	Regular cyberattack simulations (e.g., Red Teaming) help identify and mitigate security vulnerabilities.
Artificial Intelligence (AI)	AI1	Automatic updates of global threat intelligence databases are performed in real time.
	AI2	Artificial Intelligence assists in analyzing large volumes of data to predict potential cyberattacks.
	AI3	Automated defense systems can take preventive actions without manual intervention.
	AI4	Machine Learning technologies help reduce false security alerts and improve threat detection efficiency.
	AI5	Automated security updates reduce the likelihood of cyberattacks and system misuse.
	AI6	AI-based security systems are more capable of handling zero-day threats.

Vulnerability Assessment (VA)	VA1	Vulnerability assessments are conducted continuously rather than only after major updates.
	VA2	Security vulnerabilities are prioritized based on future risk predictions rather than historical incidents alone.
Readiness (RD)	RD1	Security policies prioritize prevention before incident response.
	RD2	Team members are encouraged to report anomalies as a preventive measure.
	RD3	Investment in preventive cybersecurity technologies is considered a priority.
	RD4	Continuously updated security systems improve readiness against emerging threats.
	RD5	Transparency regarding security weaknesses helps prevent cyber threats before they occur.

E. Validity and Reliability Testing

Prior to the main data analysis, validity and reliability tests were conducted to ensure the quality of the research instrument. The validity test was performed using Pearson Product-Moment Correlation to determine the extent to which each questionnaire item measured the intended construct. An item was considered valid if the correlation coefficient exceeded the critical value and the significance level was below 0.05.

The reliability test was conducted using Cronbach's Alpha coefficient to evaluate the internal consistency of the questionnaire. A Cronbach's Alpha value greater than 0.70 indicates that the instrument has acceptable reliability and can consistently measure the research variables. These tests were performed before conducting the descriptive statistical analysis. According to Nunnally and Bernstein, a Cronbach's Alpha value above 0.70 indicates acceptable reliability.

F. Data Analysis Technique

Prior to the descriptive statistical analysis, Exploratory Data Analysis (EDA) was conducted to examine respondent demographics, identify response distributions, detect potential anomalies, and ensure data completeness. EDA is a preliminary analytical approach used to understand data characteristics, identify patterns, and support subsequent statistical analysis through data exploration and summarization [29].

The collected data were analyzed using descriptive statistical analysis. The analysis aimed to describe respondents' perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy.

Descriptive statistics were used to summarize respondents' responses for each research variable, namely Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), Vulnerability Assessment (VA), and

Readiness (RD). The analysis focused on calculating the frequency distribution, percentage, and mean score of each indicator and construct.

The mean values were interpreted using the following scale: 1.00–1.80 (Strongly Disagree), 1.81–2.60 (Disagree), 2.61–3.40 (Neutral), 3.41–4.20 (Agree), and 4.21–5.00 (Strongly Agree). Higher mean scores indicate stronger positive perceptions and greater readiness toward the adoption of proactive cybersecurity practices. The results were then interpreted and discussed to provide insights into public perceptions and readiness regarding the implementation of Preemptive Cybersecurity.

III. RESULTS AND DISCUSSION

Prior to conducting descriptive statistical analysis, the validity and reliability of the research instrument were first tested to ensure the quality of the data obtained. The validity test used Pearson Product Moment Correlation, while the reliability test used Cronbach's Alpha. The test results showed that all questionnaire items met the requirements for good validity and reliability, thus declaring the research instrument worthy of further analysis.

A. Validity and Reliability Test

TABLE II
ITEM VALIDITY TEST RESULTS

Item	Corrected Item-Total Correlation	Status
Q1	0.468	Valid
Q2	0.605	Valid
Q3	0.489	Valid
Q4	0.490	Valid
Q5	0.744	Valid
Q6	0.788	Valid
Q7	0.857	Valid
Q8	0.712	Valid
Q9	0.586	Valid
Q10	0.580	Valid
Q11	0.727	Valid
Q12	0.600	Valid
Q13	0.787	Valid
Q14	0.710	Valid
Q15	0.666	Valid
Q16	0.768	Valid
Q17	0.679	Valid
Q18	0.468	Valid
Q19	0.668	Valid
Q20	0.639	Valid

Criteria: An item is declared valid if the Corrected Item-Total Correlation value > 0.30.

TABLE III
RELIABILITY TEST RESULTS

Variable	Cronbach's Alpha	Interpretation
Questionnaire Instrument	0.942	Excellent Reliability

Prior to the descriptive statistical analysis, validity and reliability tests were conducted to evaluate the quality of the research instrument. The validity test results showed that all questionnaire items achieved corrected item-total correlation values ranging from 0.468 to 0.857, exceeding both the minimum threshold of 0.30 and the r-table value of 0.294 ($n = 45$, $\alpha = 0.05$). Therefore, all items were considered valid and suitable for further analysis.

The reliability test yielded a Cronbach's Alpha value of 0.942, which is higher than the recommended threshold of 0.70. This result indicates excellent internal consistency and reliability of the questionnaire. Consequently, the instrument was deemed appropriate for measuring respondents' perceptions and readiness toward the implementation of Preemptive Cybersecurity.

B. Respondent Demographics

A total of 45 valid responses were collected and analyzed. The demographic profile of respondents is presented in Table IV.

TABLE IV
RESPONDENT DEMOGRAPHIC PROFILE

Variable	Category	Frequency	Percentage (%)
Age	< 20 years	17	37.8
	20–30 years	25	55.6
	31–40 years	2	4.4
	51–80 years	1	2.2
Gender	Male	28	62.2
	Female	17	37.8
Education	SMA/SMK	32	71.1
	Diploma (D3)	2	4.4
	Bachelor (S1)	9	20.0
	Postgraduate (S2/S3)	2	4.4

The demographic profile of respondents is presented in Table IV, most respondents were aged between 20 and 30 years (55.6%), followed by respondents under 20 years old (37.8%). Male respondents accounted for 62.2% of the sample, while female respondents represented 37.8%. The majority of respondents had a senior high school or vocational school educational background (71.1%), indicating that the sample was dominated by young and digitally active individuals.

C. Descriptive Analysis of Research Variables

Descriptive statistical analysis was conducted to evaluate respondents' perceptions regarding the implementation of Preemptive Cybersecurity. The mean score of each construct is shown in Table V.

TABLE V
DESCRIPTIVE ANALYSIS RESULTS

Variable	Number of Items	Mean Score	Interpretation
CTI	4	3.72	Agree
TH	3	3.90	Agree
AI	6	3.79	Agree
VA	2	3.74	Agree
RD	5	4.06	Agree
Overall Mean	20	3.84	Agree

Table V indicates that all research variables achieved mean scores above 3.50, reflecting positive perceptions toward the implementation of Preemptive Cybersecurity. The highest mean score was obtained by the Readiness (RD) construct (4.06), suggesting that respondents generally feel prepared to support proactive cybersecurity practices. Cyber Threat Intelligence (CTI) obtained the lowest mean score (3.72), although it still falls within the agreement category.

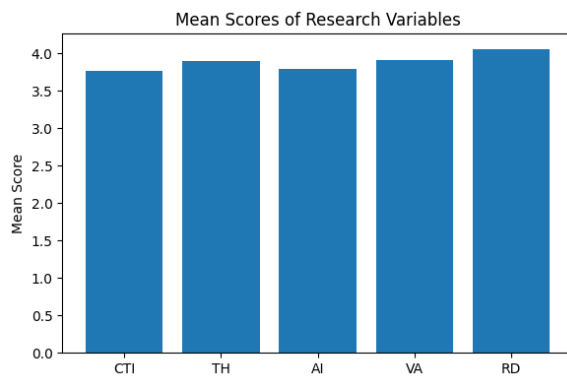


Figure 3. Mean Scores of Research Variables

Figure 3 presents the average scores of the research variables. Overall, respondents showed positive perceptions toward the implementation of Preemptive Cybersecurity.

D. Key Indicator Analysis

To identify the strongest and weakest perceptions among respondents, several indicators were examined based on their mean scores.

TABLE VI
HIGHEST AND LOWEST SCORING INDICATORS

Indicator	Mean
Team members are responsible for reporting anomalies as a preventive measure	4.31
Transparency regarding security weaknesses helps prevent cyber threats	4.16
Continuously updated security systems improve readiness against emerging threats	4.11
Availability of systems capable of detecting suspicious activities before cyberattacks occur	3.36
AI-based systems against Zero-Day threats	3.51
Systems capable of recognizing attacker behavior patterns	3.53



Figure 4. Readiness Indicator Scores

Figure 4 presents the mean scores of the readiness indicators (RD1–RD5). The results indicate that respondents generally demonstrated a relatively high level of readiness toward the implementation of Preemptive Cybersecurity practices, as all indicators achieved mean scores close to or above 4.0.

Among the readiness indicators, RD2 obtained the highest mean score, indicating strong agreement regarding organizational preparedness for proactive cybersecurity implementation. High scores were also observed for RD4 and RD5, suggesting positive perceptions of organizational support and continuous improvement efforts in cybersecurity practices.

Meanwhile, RD3 recorded the lowest mean score among the readiness indicators. Although its score remained within the agreement range, the result suggests that certain aspects of organizational readiness still require further improvement. Overall, the findings demonstrate that respondents perceive their organizations as generally prepared to adopt Preemptive Cybersecurity strategies.

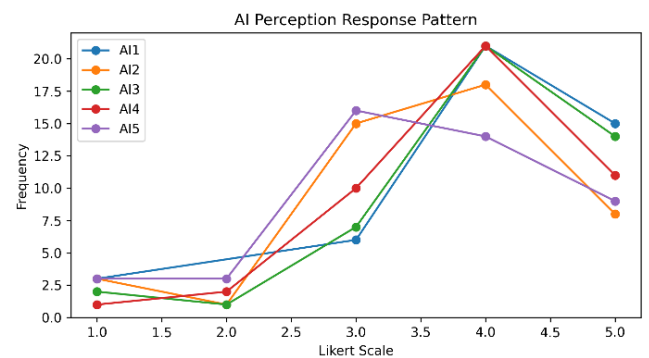


Figure 5. AI Perception Response Pattern

Figure 5 illustrates the response distribution patterns for the Artificial Intelligence (AI) indicators. Most responses were concentrated in the Agree and Strongly Agree categories, indicating positive perceptions regarding the role of AI in supporting proactive cybersecurity practices.

E. Discussion

The findings indicate that respondents generally have positive perceptions toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. The overall mean score of 3.84 demonstrates that proactive cybersecurity approaches are considered important in addressing the increasing complexity of cyber threats.

The relatively high score of the Threat Hunting construct (3.90) suggests that respondents recognize the value of actively searching for potential threats before they evolve into serious security incidents. Similarly, respondents expressed positive perceptions regarding the use of Artificial Intelligence (3.79), indicating confidence in AI-assisted threat detection, predictive analysis, and automated security responses.

The highest construct score was observed in the Readiness dimension (4.06), demonstrating that respondents generally feel prepared to support preventive cybersecurity initiatives. In particular, respondents strongly agreed that reporting anomalies, maintaining transparency, and continuously updating security systems are essential components of cybersecurity preparedness.

Overall, the results suggest that Cyber Threat Intelligence, Threat Hunting, Artificial Intelligence, and organizational readiness are positively perceived as important dimensions supporting the implementation of Preemptive Cybersecurity. These findings indicate growing awareness of proactive cybersecurity practices and their role in strengthening cyber resilience against future threats. It is important to emphasize that this study measured perceptions and self-reported readiness rather than the actual effectiveness of Preemptive Cybersecurity implementation. Therefore, conclusions regarding improved cyber resilience or the effectiveness of preemptive strategies remain provisional and should not be overstated. Positive perceptions and readiness constitute necessary but not sufficient conditions for successful implementation; empirical evaluation of outcomes (such as reduced incident rates, faster detection times, or improved resilience metrics) would require different research designs, such as longitudinal or experimental studies.

This study has several limitations. First, the number of respondents was relatively limited ($n = 45$), which may affect the generalizability of the findings. Second, the study relied on self-reported perceptions collected through questionnaires, which may introduce subjective bias. Future studies are encouraged to involve larger and more diverse samples and apply advanced statistical techniques to further validate the findings. Despite these limitations, the findings offer several practical implications for organizations seeking to advance Preemptive Cybersecurity strategies. First, the consistently high scores on readiness indicators—particularly anomaly reporting, transparency about security weaknesses, and continuous system updates—suggest that organizations can usefully invest in building a security culture that encourages early reporting, open discussion of vulnerabilities, and regular technology refresh cycles. Second, the relatively

lower (though still positive) scores on certain technical indicators, such as pre-attack detection capability and AI-based zero-day handling, indicate potential priority areas for capability development and awareness raising. Third, organizations may use the five-dimension framework (CTI, TH, AI, VA, and RD) as a structured checklist when assessing their current preemptive posture and identifying gaps between technical capability and organizational readiness. Fourth, given that readiness scored highest, leadership attention to policy orientation toward prevention, investment prioritization, and cultural enablers may yield complementary benefits alongside technical investments. These implications are suggestive rather than prescriptive and should be adapted to specific organizational contexts and validated through further research and pilot implementations.

IV. CONCLUSION

This study examined respondents' perceptions and readiness toward the implementation of Preemptive Cybersecurity as a cyber threat prevention strategy. The findings indicate that respondents generally have positive perceptions regarding proactive cybersecurity practices and recognize the importance of preventive approaches in addressing emerging cyber threats.

The descriptive analysis showed that Cyber Threat Intelligence (CTI), Threat Hunting (TH), Artificial Intelligence (AI), and Readiness (RD) are perceived as important dimensions supporting the implementation of Preemptive Cybersecurity. Respondents particularly emphasized the importance of anomaly reporting, organizational transparency, and continuously updated security systems in strengthening cybersecurity preparedness. The findings indicate that organizational readiness plays an important role in supporting the successful adoption of Preemptive Cybersecurity practices.

Overall, the findings suggest that proactive cybersecurity strategies are increasingly recognized as essential for improving cyber resilience and supporting preventive security measures. Future research is recommended to involve a larger number of respondents and apply more advanced analytical methods to further explore public perceptions and readiness toward Preemptive Cybersecurity implementation.

REFERENCES

- [1] B. Zhang, Y. Gao, B. Kuang, C. Yu, A. Fu, and W. Susilo, "A Survey on Advanced Persistent Threat Detection: A Unified Framework, Challenges, and Countermeasures," *ACM Comput. Surv.*, vol. 57, no. 3, pp. 62:2-62:36, 2024, doi: 10.1145/3700749.
- [2] S. Berrios, D. Leiva, B. Olivares, H. Allende-Cid, and P. Hermosilla, "Systematic Review: Malware Detection and Classification in Cybersecurity," *Appl. Sci.*, vol. 15, no. 14, pp. 1–32, 2025, doi: 10.3390/app15147747.
- [3] P. Radanliev, "Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing," *J. Cyber Secur. Technol.*, vol. 9, no. 1, pp. 28–78, 2025, doi:

- 10.1080/23742917.2024.2312671.
- [4] S. AboulEla, N. Ibrahim, S. Shehmir, A. Yadav, and R. Kashef, "Navigating the Cyber Threat Landscape: An In-Depth Analysis of Attack Detection within IoT Ecosystems," *AI*, vol. 5, no. 2, pp. 704–732, 2024, doi: 10.3390/ai5020037.
 - [5] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, pp. 1–20, 2023, doi: 10.3390/s23156666.
 - [6] A. I. Jony and S. A. Hamim, "Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age," *J. Inf. Technol. Cyber Secur.*, vol. 1, no. 2, pp. 53–67, 2023, doi: 10.30996/jitcs.9715.
 - [7] P. Nespoli, S. B. Molina, P. Beltran-Lopez, and F. G. Marmol, "Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision," *IEEE Commun. Surv. Tutorials*, vol. 28, pp. 1557–1596, 2025, doi: 10.1109/COMST.2025.3583868.
 - [8] N. Kshetri, "Transforming cybersecurity with agentic AI to combat emerging cyber threats," *Telecomm. Policy*, vol. 49, no. 6, p. 102976, 2025, doi: 10.1016/j.telpol.2025.102976.
 - [9] A. Tanikonda, B. K. Pandey, S. R. Peddinti, and S. R. Katragadda, "Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems," *SSRN Electron. J.*, vol. 3, no. 1, pp. 196–217, 2025, doi: 10.2139/ssrn.5102358.
 - [10] S. Ryu, J. Kim, N. Park, and Y. Seo, "Preemptive prediction-based automated cyberattack framework modeling," *Symmetry (Basel)*, vol. 13, no. 5, 2021, doi: 10.3390/sym13050793.
 - [11] Rakibul Hasan Chowdhury, Nayem Uddin Prince, Salman Mohammad Abdullah, and Labonno Akter Mim, "The role of predictive analytics in cybersecurity: Detecting and preventing threats," *World J. Adv. Res. Rev.*, vol. 23, no. 2, pp. 1615–1623, 2024, doi: 10.30574/wjarr.2024.23.2.2494.
 - [12] J. Yu, A. V. Shvetsov, and S. Hamood Alsamhi, "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions," *IEEE Access*, vol. 12, no. October, pp. 159579–159596, 2024, doi: 10.1109/ACCESS.2024.3482987.
 - [13] S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, "Cyber-threat intelligence for security decision-making: A review and research agenda for practice," *Comput. Secur.*, vol. 132, p. 103352, 2023, doi: 10.1016/j.cose.2023.103352.
 - [14] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," *Sensors*, vol. 23, no. 16, pp. 1–27, 2023, doi: 10.3390/s23167273.
 - [15] N. Sun *et al.*, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 3, pp. 1748–1774, 2023, doi: 10.1109/COMST.2023.3273282.
 - [16] B. Nour, M. Pourzandi, and M. Debbabi, "A Survey on Threat Hunting in Enterprise Networks," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 4, pp. 2299–2324, 2023, doi: 10.1109/COMST.2023.3299519.
 - [17] S. R. Sindiramutty, "Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence," *J. Artic.*, 2023, doi: <https://doi.org/10.48550/arXiv.2401.00286>.
 - [18] B. Kayode, N. T. Adebola, S. Akerele, O. Fagbohun, C. Agbo, and O. Bantale, "Journal of Artificial Intelligence , Machine Learning and Data Science The State of AI-Driven Cybersecurity : Trends , Challenges and Opportunities," *URF Publ.*, vol. 3, no. 2, pp. 1–9, 2025, doi: doi.org/10.51219/JAIMLD/Bisola-Kayode/577 Journal.
 - [19] A. Mishra, "Ai-Powered Cybersecurity Framework for Secure Data Transmission in Iot Network," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 3, pp. 05–13, 2025, doi: 10.35629/5252-07030513.
 - [20] K. Bennouk, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, A. Z. Faroukhi, and D. Mahouachi, "A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies," *J. Cybersecurity Priv.*, vol. 4, no. 4, pp. 853–908, 2024, doi: 10.3390/jcp4040040.
 - [21] P. Cheimonidis and K. Rantos, "Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review," *Futur. Internet*, vol. 15, no. 10, 2023, doi: 10.3390/fi15100324.
 - [22] A. Amulya, K. S. Swarup, and R. Ramanathan, "Cyber Security of Smart-Grid Frequency Control: A Review and Vulnerability Assessment Framework," *ACM Trans. Cyber-Physical Syst.*, vol. 8, no. 4, 2024, doi: 10.1145/3661827.
 - [23] M. Neri, F. Niccolini, and L. Martino, "Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment," *Inf. Comput. Secur.*, vol. 32, no. 1, pp. 38–52, 2024, doi: 10.1108/ICS-05-2023-0084.
 - [24] Berlilana, T. Noparumpa, A. Ruangkanjanases, T. Hariguna, and Sarmini, "Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness," *Sustain.*, vol. 13, no. 24, 2021, doi: 10.3390/su132413761.
 - [25] R. Agyemang, S. Furnell, and T. Muller, "A Context-Aware Cybersecurity Readiness Assessment Framework for Organisations in Developing and Emerging Environments," *Futur. Internet*, vol. 18, no. 4, pp. 1–30, 2026, doi: 10.3390/fi18040178.
 - [26] Dimas Febriawan and Hizra Marisa, "Understanding Indonesia's Cyber Security Policies: Opportunities and Challenges In The Digitalization Transformation Era," *JOELS J. Elect. Leadersh.*, vol. 5, no. 1, pp. 13–21, 2024, doi: 10.31849/joels.v5i1.15908.
 - [27] A. I. Saleh and M. D. Winata, "Indonesia's Cyber Security Strategy: Problems and Challenges," *IJCAH*, vol. 2023, no. Ijcah 2023, pp. 1675–1696, 2023, doi: 10.2991/978-2-38476-152-4_169.
 - [28] M. Neri, F. Niccolini, and R. Pugliese, "Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey," *Online J. Appl. Knowl. Manag.*, vol. 10, no. 2, pp. 1–22, 2022, doi: 10.36965/ojakm.2022.10(2)1-22.
 - [29] K. Hasan, "Quantitative Methods in Social Science Research: Systematic Review of Content Analysis, Survey and Experiment Methodologies," *SSRN Electron. J.*, 2024, doi: 10.2139/ssrn.4698175.
 - [30] W. Febriani, S. E. Prasty, B. Sabella, and F. D. Marleny, "Analysis of the Impact of Violent Content on Social Media on Adolescent Cyberpsychology Using Support Vector Machine and Random Forest," *J. Appl. Informatics Comput.*, vol. 10, no. 1, pp. 707–711, 2026, doi: <https://doi.org/10.30871/jaic.v10i1.11415>.