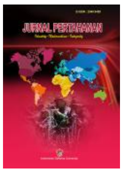


Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 11 No. 1 (2025) pp.1-15
https://jurnal.idu.ac.id/index.php/defensejournal

National Cyber Defense: Analysis of Incident Severity Factors Using a Decision Tree

Reyhan Fakhreja[1*], Khaerul Umam[2], Kamila Zahra[3], Imat Siti Nurjiah[4]
[1,2,3,4] UIN Sunan Gunung Djati Bandung, Indonesia

reyhanfakhreja@gmail.com[1*], umam@uinsgd.ac.id[2], kamilazahraa8@gmail.com[3], imatsitinurjiah29@gmail.com[4]
*Corresponding Author

Article Info

Article history:
Received: December 3, 2024
Revised: February 24, 2025
Accepted: April 30, 2025

Keywords:
Cybersecurity,
Decision Tree Classification,
Digital Infrastructure,
National Defense,
National Security Strategy

Abstract

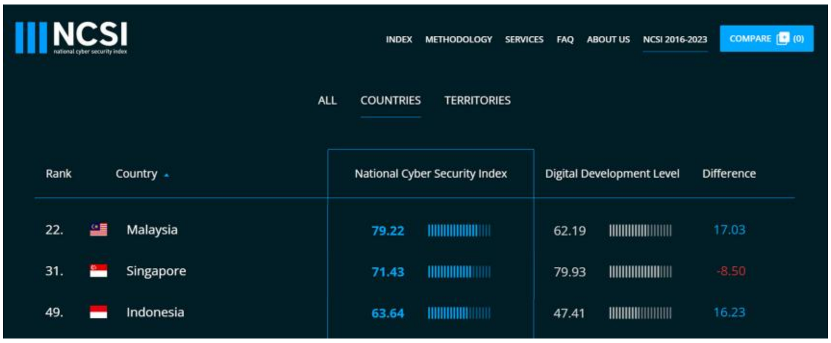
Cybersecurity became Indonesia's national defense priority after the April 2024 ransomware attack on critical infrastructure exposed systemic vulnerabilities. Despite BSSN's establishment, inter-agency coordination remains fragmented, and response delays persist. This study aims to identify the key determinants of cyber-incident severity and propose data-driven policy recommendations. A descriptive quantitative approach was applied to all 77 incidents recorded by BSSN from January to September 2024 a period chosen because it follows new regulatory measures introduced at the start of 2024 and includes multiple high-profile events. BSSN data were cross-referenced with Kominfo and Id-SIRTII logs (revealing an 8 percent discrepancy) to enhance validity. Preprocessing involved removing non-contributory fields, grouping by attack type, sector, and severity, converting categorical variables (Incident Type, Sector, Origin, Mitigation Measures, Response Time, Status) into factors, and stratified splitting into 80 percent training and 20 percent testing subsets. A decision tree model in RStudio (pruned with cp = 0.05) yielded 93.75 percent accuracy, validated by 10-fold cross-validation (mean accuracy 92.5 percent, SD 2.1 percent). Results show Incident Type as the strongest predictor of severity, followed by Mitigation Measures and Response Time. Attacks responded to within 24 hours seldom exceed medium severity, whereas delays over 48 hours, especially for exploits, Trojans, and malware, almost always result in critical outcomes. Additionally, incidents from the United States and Singapore disproportionately target underdeveloped infrastructure and governance sectors, increasing severity. To bolster Indonesia's cybersecurity resilience, recommendations include: expanding secure, evenly distributed digital infrastructure; establishing and reinforcing provincial CSIRTs; enforcing uniform audit and certification standards; and integrating digital literacy into education. Ultimately, deepening ASEAN CERT integration through synchronized incident classification and real-time threat attribution will bridge national and regional defense gaps, thereby enhancing cross-border response capabilities.

DOI:
http://dx.doi.org/10.33172/jp.v11i1.19798

INTRODUCTION

Cybersecurity has increasingly become one of the primary priorities in national defense in the ever-evolving digital age. Cyber threats are no longer merely regarded as equivalent to traditional military threats; they are becoming more complex and dynamic. This situation creates an urgent need for adaptive and comprehensive national defense policies to address these cyber threats. Previous research has highlighted the importance of cybersecurity as a strategic element in safeguarding the country's digital assets, including critical infrastructure and sensitive information. This concept involves the integration of technical, institutional, and policy aspects, all of which are interrelated in countering threats such as hacking attacks, malware, and data breaches, which may have far-reaching implications for national security (Ginanjar, 2022).

In the subject of data security, theoretically, classification methods, including decision trees, have been extensively applied to detect and model the degrees of event severity. While Han et al. (2012) underlined the benefits of decision trees in expressing links between variables intuitively and hierarchically, Quinlan (1986) presented the C4.5 algorithm, which evolved into the forerunner of contemporary decision trees. The application of this classification model in several cybersecurity research studies by Mansur & Zaman (2023) and Messaoud et al. (2016) which reveals that decision trees are efficient in forecasting risk categories and help in the design of targeted mitigating actions.



Rank	Country	National Cyber Security Index	Digital Development Level	Difference
22.	Malaysia	79.22	62.19	17.03
31.	Singapore	71.43	79.93	-8.50
49.	Indonesia	63.64	47.41	16.23

Figure 1. National Cyber Security Index 2024 (NCSI, 2024)

According to data from the BSSN report, between January and September 2024, there was a high incidence of cyber threats, with over 147 million anomalous traffic events and more than 1 million Advanced Persistent Threat (APT) incidents. These cases underscore the urgent need for more effective strategies to safeguard critical digital infrastructure and enhance Indonesia's position in the National Cybersecurity Index, which currently ranks 49th, far behind neighboring countries such as Malaysia and Singapore (NCSI, 2024). Notwithstanding Indonesia's initiatives in cybersecurity via the formation of the National Cyber and Encryption Agency (BSSN), the nation persists in confronting significant cyber threats, intensified by sluggish incident response times, inadequate inter-agency collaboration, and infrastructural constraints. There is a lack of comprehensive research on how national defense strategies effectively mitigate cyber threats.

There is a clear research gap regarding how an integrated national defense strategy encompassing institutional, technical, and regulatory aspects effectively reduces the severity of cyber incidents in Indonesia. Previous studies have focused more on each component separately, thus failing to provide a comprehensive picture of the determinants of incident severity. Numerous studies have been conducted on cybersecurity. However, a variation in focus still exists, indicating space for broader integration. Some studies emphasize the role of the National Cyber and Encryption Agency (BSSN) in building national cybersecurity (Ginanjar, 2022), while others highlight the challenges in securing data within cyberspace and the importance of strengthening institutional roles to build an effective defense system in the digital era (Azzahrah et al., 2024). Nevertheless, research specifically addressing the comprehensive implementation of national defense policy in countering cyber threats, encompassing institutional, technical, and legal regulatory aspects, remains limited (Witarti & Armandha, 2018).

Therefore, this research explicitly fills that gap by integrating institutional, technical, and regulatory aspects into a single analytical framework, utilizing a decision tree model to identify key factors influencing the severity of cyber incidents in Indonesia and formulate holistic policy recommendations. This data-driven strategy not only provides strategic insights for creating a more comprehensive and adaptable cybersecurity policy but also facilitates the effective execution of national defense operations. Ultimately, the outcomes should significantly complement the national defense plan and serve as the primary direction for Indonesia in managing the increasingly complex and dynamic character of cyber threats in the digital age.

METHODS

This study employs a descriptive quantitative approach to analyze the vulnerability of critical sectors in Indonesia to cyber threats. This approach was chosen because it provides measurable and objective results, as well as identifies patterns and relationships between variables within complex systems, which is crucial for understanding the factors influencing the severity of cyber incidents (Creswell & Creswell, 2018). Through this approach, the study is expected to provide a comprehensive overview of the factors that affect the severity of cyber incidents.

Data source

The primary data for this study were obtained from the official reports of the National Cyber and Encryption Agency (BSSN), which recorded cyber incidents from January to September 2024. The January–September 2024 timeframe was selected because it corresponds with BSSN's standardized reporting period, during which several high-profile incidents, such as the April ransomware attack on national infrastructure, highlighted urgent vulnerabilities. By focusing on this specific interval, the study can contextualize findings within recent regulatory changes implemented at the start of 2024. Although there are just 77 recorded observations, this dataset includes all cyber events documented by BSSN from January to September 2024, making it comprehensive for that timeframe. The varied diversity of attack kinds and impacted industries ensures a thorough depiction of incidence severity trends across several crucial areas. To mitigate potential inaccuracies inherent to a single source, this research also cross-references data from the Ministry of Communication and Digital (Kominfo) and the Indonesian Security Incident Response Team Forum (Id-SIRTII). Kominfo's Government CSIRT (Govt-CSIRT) aggregates incidents primarily through ISP-level monitoring and public reporting mechanisms (Direktorat Jenderal Infrastruktur Digital, 2013).

Whereas Id-SIRTII performs continuous network-node logging and threat intelligence sharing among private-sector stakeholders (Komdigi, 2006). A preliminary comparison of the two sources for Q1–Q2 2024 indicates that Id-SIRTII's logs report approximately 8% more incidents than Kominfo's Govt-CSIRT data, underscoring the importance of multi-source validation. These methodological differences and their impact on incident counts will be discussed further in the Limitations section. In addition, the decision tree methodology has demonstrated its stability on datasets of small to medium size, provided that the variables have been meticulously processed through rigorous preprocessing (Han et al., 2012). The dataset consists of 77 observations, covering various types of cyberattacks, such as Malware, Trojan, Exploit, and others, as well as the affected sectors, including Government, Finance, and Telecommunications. The data also includes information regarding the number of incidents recorded for each type of attack and the sectors involved. The report provides a comprehensive overview of the mitigation measures implemented, as well as the response times to the incidents. Additionally, to offer a broader perspective, supplementary data were obtained from the National Cyber Security Index (NCSI), which illustrates Indonesia's position in the global cybersecurity context.

Preprocessing Data

Before the analysis was conducted, the data underwent several preprocessing stages to ensure the quality of the data used was both valid and relevant.

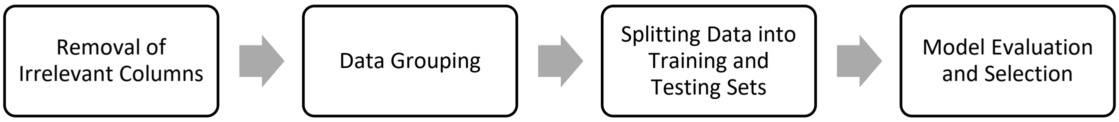

Removal of Irrelevant Columns
Data Grouping
Splitting Data into Training and Testing Sets
Model Evaluation and Selection

Figure 2. Data Preprocessing Flow (Han et al., 2012a)

The first step involved removing irrelevant columns, such as those that did not directly contribute to the analysis. Next, the data were grouped based on attack type, affected sectors, and the severity of the incidents. Subsequently, categorical variables, such as Incident Type, Affected Sectors, Country of Origin (Attack), Mitigation Measures, Response Time, and Incident Status, were converted into factor data types to facilitate processing within the decision tree model, allowing for more precise identification of patterns between variables. Finally, the dataset was divided into two subsets 80% for training and 20% for testing to evaluate the model's performance.

The training set (80% of observations) was used to build and tune the decision tree model, learning relationships and patterns among predictors. The testing set (20%) served as unseen data to assess the model's ability to generalize; it was not exposed to the model during training. A stratified random sampling approach was applied to maintain the original distribution of severity categories across both subsets, ensuring that each class (Critical, High, Medium, Low) was adequately represented in training and testing. This two-category split is common practice in predictive analysis to balance the need for sufficient data to train the model while preserving an independent portion for unbiased evaluation (Han et al., 2012).

Analytical Techniques

After the preprocessing stage, the data were analyzed using decision tree classification techniques, which were chosen for their ability to present relationships between variables in a hierarchical structure that is easy to understand (Quinlan, 1986). This technique also has strong predictive capabilities for identifying key factors influencing the severity of cyber incidents. The analysis process began by dividing the dataset, which consisted of 77 observations, into 80% training data and 20% testing data. A decision tree model was built using the training data and fine-tuned through pruning with a cp parameter set to 0.05 to reduce model complexity and prevent overfitting. Model validation was performed by comparing the predicted results with actual values from the testing data, yielding an accuracy rate of 93.75%. All analyses were performed using RStudio software, which supports the implementation of decision tree techniques. The final results were visualized in the form of a decision tree to facilitate interpretation by policymakers, highlighting key variables such as attack type (X1), mitigation measures (X5), and incident response time (X6). This visualization aids in understanding the most significant factors in determining the severity of cyber incidents.

Model Validation

The model's accuracy was measured at 93.75%, and it was further verified by 10-fold cross-validation to confirm performance stability. The cross-validation results indicated an average accuracy of 92.5% with a standard deviation of 2.1%. Subsequent analysis of the confusion matrix facilitates the computation of precision, recall, and F1-score for each severity category. The F1-score for the Critical class was 0.85, and the overall AUC-ROC was 0.94, confirming the model's efficacy in differentiating across severity categories (Dunham, 2008; Quinlan, 1986).

Evaluation of Results

Confusing the model's predictions with the test data using a confusion matrix helped one evaluate the results. The used assessment tools cover accuracy, sensitivity, specificity, positive predictive value, and negative predictive value. With a 93.75% accuracy rate, the decision tree model showed remarkable performance. The model attained a sensitivity of 100% in identifying events categorized as Critical, Medium, and Low severity; yet, the sensitivity for the High severity category was noted at 66.67%, suggesting possible improvement (Han et al., 2012). With results of 91.67% for the Critical class and 100% for both the Low and Medium classes, the model showed outstanding specificity. Additionally, the model’s performance was further assessed using ROC Curve analysis to evaluate the trade-off between false positives and true positives, which is essential in classification problems (Dunham, 2008). This evaluation demonstrates that the decision tree model can provide relevant and reliable results to support strategic decision-making related to cybersecurity in critical sectors in Indonesia.

RESULT AND DISCUSSION

Data Description

This study analyzes cyber incidents reported by the National Cyber and Encryption Agency (BSSN) during the period from January to September 2024. The dataset consists of seven main variables, namely Incident Type, Number of Incidents, Affected Sectors, Country of Origin (Attack), Mitigation Measures, Response Time, and Incident Status. The most frequently reported types of attacks were Malware, Trojan Activity, and Information Leak.

Table 1. Reported Attack Types from January to September 2024. Processed by the Author from BSSN (2024)

Attack Type	Total
Malware	89,372,425
Trojan	27,759,283
Information Leak	8,533,479

Furthermore, many attack vectors, including Exploits, Web Application Attacks, Advanced Persistent Threats (APT), Denial-of-Service (DoS), and Information Gathering, present considerable risks. The Government Administration sector was the most frequently targeted, exhibiting a greater number of events than other sectors (BSSN, 2024). The countries with the highest frequency of attacks are Indonesia (50 million), the United States (12.1 million), Singapore (3.2 million), Bulgaria (3.1 million), and the Netherlands (1.8 million). The response time to occurrences varied between 12 and 72 hours, with an average of 36 hours. The majority of events have been resolved, while the other cases are currently under investigation or ongoing (BSSN, 2024).

Decision Tree Model Result

It should be noted that this decision tree model is predictive and reveals associative patterns (correlation) between input variables and the severity level of incidents, but does not directly prove causal relationships. Further interpretation requires experimental studies or separate causality analysis (Willig et al., 2021; Y & Pandian, 2021; Zhang et al., 2024). The decision tree model was constructed by splitting the data into 80% training data and 20% test data. After pruning using a complexity parameter (cp) value of 0.05, the model achieved a final accuracy of 93.75%.

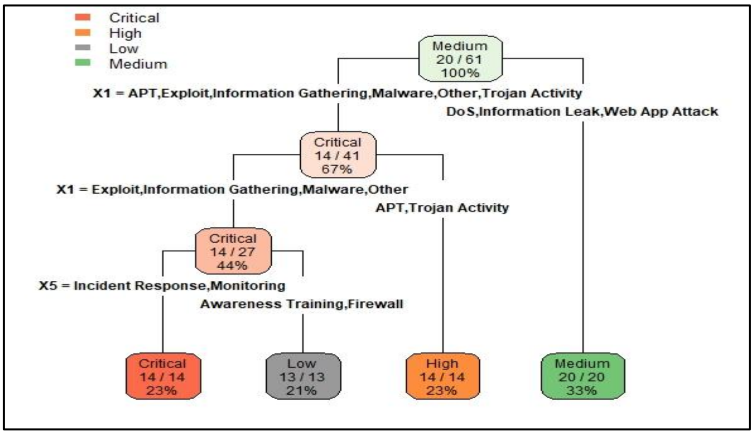

Critical
High
Low
Medium
Medium 20 / 61 100%
X1 = APT,Exploit,Information Gathering,Malware,Other,Trojan Activity
DoS,Information Leak,Web App Attack
Critical 14 / 41 67%
X1 = Exploit,Information Gathering,Malware,Other
APT,Trojan Activity
Critical 14 / 27 44%
X5 = Incident Response,Monitoring
Awareness Training,Firewall
Critical 14 / 14 23%
Low 13 / 13 21%
High 14 / 14 23%
Medium 20 / 20 33%

Figure 3. Decision Tree Model Test Result (Processed by the Author, 2024)

With Mitigating Measures ranked closely behind, the final model shows that the Incident Type variable is the most important determinant of incident severity (Purwanti, 2025). Although decisive mitigation actions, such as effective incident response and continuous monitoring, usually result in High and Critical severity ratings, Attacks marked by Exploits and Trojan Activity are relatively likely to be classified as Critical events. On the other hand, less successful approaches, such as awareness training, reconfiguration, and patching, are usually associated with Medium or Low degree outcomes. Furthermore, attack routes like malware and exploits are especially prone to be labelled as Critical when the reaction time exceeds 48 hours, therefore underlining the results of postponed interventions (Purwanti, 2025). The country of origin is very important since attacks from the United States and Singapore usually result in great severity, particularly in the Infrastructure and Government sectors (Sudarmadi & Runturambi, 2019).

The Importance of Features in Decision Tree Models

The decision tree model used in this study intrinsically generates information regarding feature importance, namely, the measure of contribution of each variable in reducing impurity (in this case, the Gini index) (Chen et al., 2023). The visualization results in Figure 4 show that AttackType (Type of Attack) is the most dominant feature, contributing about 40% of the total decision information used by the model. The following variables that make substantial contributions are Sector (Affected Sector), NumAttacks (Number of Incidents), and Mitigation, each of which contributes approximately 10–13%. In contrast, the classification procedure is comparatively less influenced by variables such as Status, response time, and origin country.

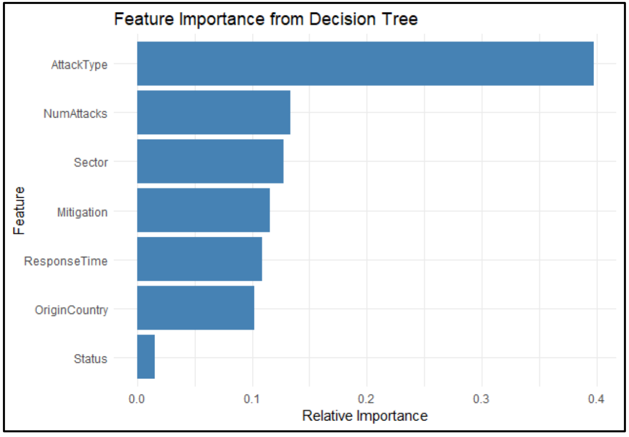


Figure 4. Visualization of the Relative Contribution of Each Feature Based on the Gini Index in the Decision Tree Model (Processed by the Author, 2024).

The importance of AttackType in this model is consistent with previous findings that certain types of attacks, such as Trojan Activity or APT, tend to be associated with high severity levels. Meanwhile, ResponseTime, which plays a substantively important role in mitigation, has a secondary role in this model, as its variation is more limited or overshadowed by the predictive power of other variables.

Model Evaluation

Using 20% of the test data, the model was evaluated and attained a final accuracy of 93.75% with a 95% confidence interval spanning from 69.77% to 99.84%. Among the evaluation measures were McNemar's Test, which gauged the statistical relevance of variations in classification performance, and Kappa statistic, which gauged the agreement between expected and actual classifications (Han et al., 2012a).

Table 2. Model Evaluation Accuracy Values (Processed by the Author, 2024)

Overall Statistics	**Value**
Accuracy	: **0.9375**
95% CI	: **(0.6977, 0.9984)**
No Information Rate	: 0.3125
P-Value [Acc > NIR]	: 2.994e-07
Kappa	: 0.9153
Mcnemar's Test P-Value	: NA

While the sensitivity for the Critical class was 91.67%, the model evaluation showed great sensitivity in spotting events with Medium and Low severity levels, both attaining 100%. Still, the High class's sensitivity at 66.67% showed space for development. Further validation of the classification efficacy of the model came from additional performance evaluation, applying the Receiver Operating Characteristic (ROC) curve (Han et al., 2012).

Table 3. Sensitivity Evaluation Values of the Model (Processed by the Author, 2024)

Statistics by Class	**Critical**	**High**	**Medium**	**Low**
Sensitivity	1.0000	0.6667	1.0000	1.00
Specificity	0.9167	1.0000	1.0000	1.00
Pos Pred Value	0.8000	1.0000	1.0000	1.00
Neg Pred Value	1.0000	0.9286	1.0000	1.00
Prevalence	0.2500	0.1875	0.3125	0.25
Detection Rate	0.2500	0.1250	0.3125	0.25
Detection Prevalence	0.3125	0.1250	0.3125	0.25
Balanced Accuracy	0.9583	0.8333	1.0000	1.00

The model demonstrates excellent performance in detecting incidents with critical severity (sensitivity of 91.67%), medium severity (sensitivity of 100%), and low severity (sensitivity of 100%). However, the model has lower sensitivity for incidents with high severity, indicating that the model is less optimal in detecting threats with moderate impact. Therefore, there is an opportunity to enhance the model's performance in better detecting high-severity threats.

Significance of Mitigation Measures as a Key Factor

This study finds that Mitigation Measures are one of the most significant variables in determining the severity of cyber incidents. Mitigation measures such as Incident Response and Monitoring have been shown to have a significant impact in reducing the severity of cyber incidents. These findings suggest that rapid and structured responsive actions can reduce the risk of incidents being categorized as Low or Medium. These findings are consistent with those of Fitriati (2016), who emphasizes that strong technological infrastructure is a fundamental foundation for addressing cyber threats. Furthermore, threats to a country's critical infrastructure can significantly disrupt both economic stability and national security. While Fitriati (2016) and Tristantri & Prasojo (2016) broadly advocate for strengthening digital infrastructure and technology-driven mitigation, our study adds novelty by providing empirical, data-driven evidence via decision tree analysis that specific infrastructure gaps (e.g., between urban and rural networks) correlate with higher incident severity. This allows policymakers to prioritize targeted investments in areas where deficiencies most strongly predict critical outcomes in key sectors, which is crucial to mitigating the potential major impacts of cyberattacks (Tristantri & Prasodjo, 2023).

However, the implementation of these mitigation measures in Indonesia continues to face challenges, particularly concerning the limited digital infrastructure in remote areas and the shortage of skilled personnel in this field. These limitations lead to vulnerabilities in managing cyber threats, particularly in the government sector and private institutions, which are primary targets for cyberattacks (Sudarmadi & Runturambi, 2019). By comparison, Singapore has integrated technical mitigation measures with national policies that require each government agency to conduct annual cybersecurity audits. Although BSSN has already established a government CSIRT network and issued audit guidelines (Azhar, 2024), actual implementation remains uneven: many regional agencies still lack standardized audit procedures, certified assessors, and clear enforcement mechanisms (Sudarmadi & Runturambi, 2019). Instead of simply mandating audits, Indonesia should focus on refining its framework by developing uniform audit standards, strengthening local CSIRTs' capacity, particularly in underserved provinces, and ensuring that identified vulnerabilities receive timely remediation and follow-up verification.

The Importance of a Prompt Response in Mitigating The Impact of Incidents

Another key finding of this study indicates that Response Time is a critical factor in determining the severity of cyberattacks. Attacks that are responded to within 24 hours tend to have a lower severity level (Medium or High), while slower responses (>48 hours) increase the likelihood of incidents escalating to Critical. This finding supports the study of Ginanjar (2022), which demonstrates that quick responses can help reduce the impact of attacks, especially in cases of ransomware attacks that threaten critical organizational data. It underscores the need to enhance the capacity of Incident Response Teams (IRT) in each critical sector.

However, this research also identifies that many public organizations in Indonesia still lack adequately trained Incident Response Teams and standardized procedures to handle cyber incidents promptly (Prabaswari et al., 2022). As of 30 September 2024, BSSN reported that 264 CSIRT units had been established across national and regional institutions, but distribution remains uneven: only 22 out of 38 provinces had fully operational CSIRTs, leaving 16 provinces without localized incident response capacity (Azhar, 2024). Provinces such as Papua Barat and Maluku Utara remain unserved, forcing affected organizations there to rely solely on the national Gov-CSIRT, which can introduce response delays exceeding 48 hours. Prabaswari et al. (2022) found that provinces without local CSIRTs experienced approximately 30 % longer average response times and a 15 % increase in incidents classified as Critical, compared to provinces with active CSIRTs (Prabaswari et al., 2022). Therefore, a strategic step is not only the establishment of new provincial CSIRTs but also strengthening existing ones in underserved areas. For example, South Korea's Korea Internet & Security Agency (KISA) serves both as a national and regional response center, with satellite branches in all major regions to ensure sub-24-hour responses (Cho, 2022). Indonesia could adopt a similar tiered structure by empowering BSSN to provide technical assistance, standardized SOPs, and regular audits to each provincial CSIRT, thereby reducing reliance on a centralized Gov-CSIRT and improving local resilience.

The Role of the Country of Origin of Attacks in Determining Severity Levels

This study also found that attacks originating from countries such as the United States and Singapore tend to have higher severity levels compared to those from other countries. This finding is consistent with research showing that state actors with high cyber capabilities, particularly those involved in Advanced Persistent Threats (APT), often target the financial and government sectors to create significant disruption and destabilize national stability (Messaoud et al., 2017). APT attacks from these countries are designed to exploit vulnerabilities in critical infrastructure that are still under development in countries like Indonesia, thus increasing the risk of incidents with large-scale impacts on national security and the economy (Mansur & Zaman, 2023). Attacks from state actors, such as APTs, are often designed to exploit complex weaknesses to disrupt national stability. In the context of Indonesia, attacks from these countries have the potential to weaken the country's digital infrastructure, which is still in the development phase.

Before discussing ASEAN-level responses, it is crucial to understand Indonesia's existing collaborative arrangements. Currently, Indonesia participates in bilateral information-sharing agreements with Singapore's Cyber Security Agency (CSA) and is a member of the ASEAN Cybersecurity Cooperation. However, these mechanisms have yet to produce a unified, real-time emergency response protocol focused on APT mitigation, resulting in fragmented intelligence sharing and slower cross-border coordination (Tay, 2023). At present, ASEAN's regional framework for cybersecurity is anchored by the ASEAN Cybersecurity Cooperation Strategy 2021–2025, which establishes the ASEAN Computer Emergency Response Team (CERT) network.

This network aims to facilitate incident reporting and threat intelligence sharing among member-state CSIRTs through the ASEAN CERT Programme. Under this programme, each ASEAN member maintains a CERT that communicates via secured channels and periodic joint exercises. For example, the ASEAN Cyber Drill exercises conducted since 2018 simulate cross-border APT scenarios to test readiness and information-exchange protocols (ASEAN Secretariat, 2022). Despite these efforts, gaps remain: real-time coordination is hindered by differing national policies on data privacy and inconsistent technical standards for reporting incidents, which can delay joint responses to high-severity threats (Tay, 2023).

Given these limitations, the strategic implication of our findings is that Indonesia should not only strengthen its bilateral and national CSIRT capabilities but also advocate for deeper integration within the ASEAN CERT framework. By proactively proposing common standard operating procedures for APT attribution, synchronized incident classification thresholds, and secure cross-border information exchanges, Indonesia can help transform ASEAN CERT from a primarily information-sharing body into an operational, coordinated response entity capable of handling sophisticated threats from high-capability origins like the United States and Singapore (Association of Southeast Asian Nations, 2022). Moreover, ASEAN has placed greater emphasis on capacity building and the development of cross-border data policies through cooperation programs with partner countries such as Japan and China. These programs aim to enhance the capabilities of member states in responding to cyber incidents and creating a secure and inclusive digital environment (ASEAN Secretariat, 2022).

Nevertheless, Tay (2023) highlights that ASEAN still requires a more integrated emergency response framework to address large-scale, cross-border attacks. Indonesia can play a more active role in strengthening this mechanism by advocating for the establishment of a coordinated cyber emergency response system and collaborating with advanced nations in the region, such as Japan, South Korea, and Singapore, which have more mature cyber capabilities. This approach can strengthen Indonesia's national cybersecurity defenses while enhancing digital security stability across Southeast Asia.

Strategic Recommendations and Policy Implications for Indonesia

Strengthening National Digital Infrastructure

Strengthening digital infrastructure is a strategic step that the Indonesian government must prioritize to enhance national cybersecurity resilience. The infrastructure gap between urban centers and remote regions remains a key barrier to creating a uniform cybersecurity ecosystem. Areas with suboptimal digital infrastructure tend to be more vulnerable to cyberattacks, particularly in critical sectors such as finance, energy, transportation, and government. Therefore, the government should expedite investment in the development of digital infrastructure, which includes providing secure and stable internet networks, establishing distributed regional data centers, and reinforcing security systems for critical national infrastructure (CNI). This approach will not only reduce vulnerabilities to cyberattacks but also improve Indonesia's position in global cybersecurity rankings, such as the National Cyber Security Index (NCSI), where the country currently lags behind neighboring nations like Singapore and Malaysia. For instance, Singapore has successfully enhanced its national cybersecurity resilience through policies that integrate digital infrastructure development with annual cybersecurity audits in critical sectors. Indonesia can create a more robust and measurable cybersecurity system by adopting a similar approach.

Enhancing Cyber Incident Response Capacity

The speed of responding to cyber incidents has proven to be a key factor in reducing the severity of attacks. As indicated by the results of this study, responses within 24 hours can significantly mitigate the impact of attacks, often reducing them to Medium or High severity levels. However, delayed responses, particularly those exceeding 48 hours, tend to increase the risk of an attack escalating to Critical levels, which can have widespread repercussions on organizational operations and reputation. To address this challenge, the government needs to establish Regional Cyber Incident Response Centers (CSIRTs) in each province. CSIRTs would serve as coordination hubs for early detection, mitigation, and post-incident recovery at the regional level. Additionally, CSIRTs could function as training platforms for incident response teams in critical sectors, providing cyberattack simulations, digital forensics skill development, and enhancing threat intelligence analysis capabilities. As a comparison, South Korea has established the Korea Internet & Security Agency (KISA), which is responsible for coordinating both national and regional cyber incident responses. Indonesia can adopt this model to strengthen its preparedness to tackle increasingly complex and diverse cyber threats (Cho, 2022).

Strengthening International Collaboration in Cybersecurity

Given the significant cyber threats posed by state actors such as the United States and Singapore, Indonesia needs to enhance international collaboration in the field of cybersecurity. This collaboration is crucial for improving technological capacity and human resources and sharing cross-border threat intelligence. Indonesia can play a more active role within the framework of the ASEAN Cybersecurity Cooperation, which aims to build an integrated regional cybersecurity defense system. Additionally, strategic partnerships with advanced nations such as South Korea, Japan, and the United States can help Indonesia improve its technological capacity and accelerate the adoption of best practices in cybersecurity. This collaboration will not only enhance early detection and cross-border response capabilities but also strengthen Indonesia's diplomatic position in addressing increasingly complex global cyber threats.

Cybersecurity Audits and Certification in Critical Sectors

Policies that mandate regular cybersecurity audits and certifications in critical sectors are strategic measures that must be implemented promptly. These audits aim to assess the preparedness of organizations to face cyber threats, ensure that mitigation measures have been effectively implemented, and identify potential security gaps that malicious actors could exploit. Cybersecurity certification could become a mandatory requirement for organizations that manage sensitive data or vital infrastructure. Such certifications should include evaluations of system security integrity, the readiness of incident response teams, and the data security policies in place. Countries like Germany and the United Kingdom have successfully enhanced their national cybersecurity resilience by implementing strict audit and certification policies in strategic sectors. With structured audits and certifications, the government can ensure that each critical sector has optimal protection, significantly minimizing the risk of cyberattacks.

Enhancing Digital Awareness and Literacy

In addition to technical measures, enhancing digital awareness and literacy among the general public and government sectors is a critical factor in improving national cybersecurity. Cyberattacks such as phishing, ransomware, and social engineering often succeed due to a lack of understanding about these threats and how to protect oneself from them. Therefore, the government should integrate digital literacy into formal education curricula and launch national cybersecurity awareness campaigns. These campaigns can be conducted in collaboration with the private sector, media, and educational institutions to reach a wide audience, especially in areas with low digital literacy levels. With improved digital literacy, the public is expected to become the first line of defense against cyber threats, thus minimizing the risk of social engineering-based attacks. The implementation of a comprehensive, data-driven policy as recommended in this study is expected to strengthen Indonesia's preparedness in dealing with increasingly complex cyber threats. By integrating infrastructure strengthening, capacity building, international collaboration, cybersecurity audits, and public education, Indonesia can enhance its national resilience in cybersecurity and strengthen its position in the global digital security landscape.

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

This study confirms that three factors, technology - driven mitigation (especially rapid incident response and continuous monitoring), incident response time, and the attack’s country of origin, are the strongest predictors of cyber-incident severity in Indonesia. Incidents responded to within 24 hours rarely escalate to critical levels, whereas delays beyond 48 hours almost invariably do. Attacks from cyber-capable states, such as the United States and Singapore, disproportionately target underdeveloped digital infrastructure, resulting in more severe outcomes. These findings validate the use of decision tree analysis on BSSN’s January–September 2024 dataset and address the study’s aim of identifying determinants of severity within Indonesia’s national defense framework. To mitigate these risks, Indonesia must accelerate investment in secure, evenly distributed digital infrastructure, particularly in provinces still lacking local CSIRTs, so that response times can be reduced nationwide. Existing audit guidelines and

CSIRT networks should be strengthened by enforcing uniform cybersecurity certification standards, providing certified assessors, and ensuring follow-up on identified vulnerabilities. Concurrently, integrating digital literacy into formal education and launching national awareness campaigns will address human-factor vulnerabilities that extend beyond technical controls. Finally, Indonesia should work to evolve ASEAN's CERT framework from an information-sharing forum into a coordinated response entity by advocating synchronized incident classification, joint threat-attribution protocols, and secure real-time exchanges, thereby closing the gap between national practices and regional readiness.

However, this study has limitations. Its reliance on 77 observations from BSSN reports may overlook unreported or emerging threats, despite cross-validation with Kominfo and Id-SIRTII data. The decision tree model identifies associations but not causality; future research should employ more advanced algorithms (such as Random Forest or neural networks) and incorporate longitudinal datasets to capture evolving patterns. Moreover, bridging Indonesia's national cybersecurity maturity with ASEAN's existing mechanisms requires empirical validation, such as case studies of cross‑border incident responses, to ensure proposed integrations are feasible and effective. By addressing these gaps, diversifying data sources, refining analytical methods, and examining regional collaboration in depth, subsequent studies can build on this work and strengthen Indonesia's resilience within both national and ASEAN contexts.

REFERENCES

ASEAN Secretariat. (2022). Chairman's Statement of the 29th ASEAN Regional Forum, Phanom Penh, Cambodia, 5 August 2022. *ASEAN Secretariat*, *August*, 1–9.

Association of Southeast Asian Nations. (2022). ASEAN Cybersecurity Cooperation Strategy (2021-2025). *asean.org*, 1–14.

Azhar, M. (2024, October). *BSSN Luncurkan Tim Tanggap Insiden Siber (CSIRT) Pemerintah Daerah*. Govinsider. https://govinsider.asia/indo-en/article/bssn-luncurkan-tim-tanggap-insiden-siber-csirt-pemerintah-daerah

Azzahrah, B. T., Naufal, M., Hamdi, R., Raynee, R., & Layla, Z. (2024). Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi. *Jurnal Pendidikan Tambusai*, *8*(2), 23934–23943.

BSSN. (2024). *Laporan Bulanan Publik Januari-September 2024*.

Chen, J., Tan, R., & Yang, Y. (2023). Research on An Innovative Feature Importance Recognition Algorithm Based on GINI-OOB Index. In IEEE (Ed.), *2023 IEEE International Conference on Image Processing and Computer Applications (ICIPCA)* (pp. 862–866). IEEE. https://doi.org/10.1109/icipca59209.2023.10257830

Cho, S. (2022). *National Cybersecurity Organisation: REPUBLIC OF KOREA*. 1–27.

Creswell, J., & Creswell, J. D. (2018). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches Fifth Edition* (H. Salmon, A. Marks, C. Neve, & D. C. Felts (eds.); Fifth). SAGE Publications, Inc.

Direktorat Jenderal Infrastruktur Digital. (2013). *Ancaman Cyber Attack Dan Urgensi Keamanan Informasi Nasional*. Direktorat Jenderal Infrastruktur Digital. https://www.postel.go.id/berita-ancaman-cyber-attack-dan-urgensi-keamanan-informasi-nasional-26-2079

Dunham, M. H. (2008). Data Mining: Introductory and Advanced Topics 1st Edition. In Pearson India (Ed.), *Pearson* (1st ed.). Pearson India.

Fitriati, R. (2016). *Membangun Model Kebijakan Nasional Keamanan Siber Dalam Sistem Pertahanan Negara* (Yono Reksoprodjo & Bambang Wahyudi (eds.); 2nd ed.).

Universitas Pertahanan Indonesia.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime melalui Badan Siber dan Sandi Negara. *Jurnal Dinamika Global*, *7*(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Han, J., Kamber, M., & Pei, J. (2012a). *Data Mining: Concept and Techniques* (Third Edit). Elsevier. https://doi.org/10.1016/C2009-0-61819-5

Han, J., Kamber, M., & Pei, J. (2012b). *Data Mining: Concepts and Techniques* (Elsevier (ed.); Third Edit). Elsevier. https://doi.org/10.1016/C2009-0-61819-5

Komdigi. (2006, November). Undangan Sosialisasi Indonesian Security Incidence Response Team on Information Infrastructure (ID-SIRTII) bagi Para Wartawan Media Massa Pada Tanggal 22 November 2006. *postel.go.id*.

Mansur, A. Al, & Zaman, T. (2023). User Behavior Analytics in Advanced Persistent Threats: A Comprehensive Review of Detection and Mitigation Strategies. *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, 1–6. https://doi.org/10.1109/isas60782.2023.10391553

Messaoud, B. I. D., Guennoun, K., Wahbi, M., & Sadik, M. (2017). Advanced Persistent Threat: New Analysis Driven by Life Cycle Phases and Their Challenges. In IEEE (Ed.), *2016 International Conference on Advanced Communication Systems and Information Security, ACOSIS 2016-Proceedings*. IEEE. https://doi.org/10.1109/ACOSIS.2016.7843932

NCSI. (2024). *49. Indonesia 63.64*. National Cyber Security Index.

Prabaswari, Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan Jurnal Inovasi Kebijakan*, *6*(1), 1–13. https://doi.org/10.21787/mp.6.1.2022.1-13

Purwanti, P. (2025). Visualisasi Data Cyber Security Attack Dengan Fitur Prediksi Serangan Dan Mitigasi Risiko:Perspektif Generative Gemini AI. *Jurnal Minfo Polgan*, *13*(2), 2340–2350. https://doi.org/10.33395/jmp.v13i2.14453

Quinlan, J. R. (1986). Induction of decision trees. *Machine Learning*, *1*(1), 81–106. https://doi.org/10.1007/bf00116251

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178. https://doi.org/10.7454/jkskn.v2i2.10028

Tay, K. L. (2023). *ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework*. The International Institute of Strategic Studies. https://www.iiss.org/research-paper/2023/06/asean-cyber-security-cooperation-towards-a-regional-emergency-response-framework/

Tristantri, C. N., & Prasodjo, H. (2023). United States National Strategy for Defending Vital Infrastructure from Cyberattacks. *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity*, *9*(3), 542–558. https://doi.org/10.33172/jp.v9i3.16970

Willig, M., Zecevic, M., Dhami, D. S., & Kersting, K. (2021). The Causal Loss: Driving Correlation to Imply Causation. *ArXiv*, *abs/2110.1*(October), 13. https://doi.org/10.48550/arXiv.2110.12066

Witarti, D. I., & Armandha, S. T. (2018). Tinjauan Teoritis Konsepsi Pertahanan dan Keamanan di Era Globalisasi Industri Pertahan. *Jurnal Pertahanan & Bela Negara*, *5*(3), 87–106. https://doi.org/10.33172/jpbh.v5i3.371

Y, S., & Pandian, S. L. (2021). Causal Discovery Using Dimensionality Reduction Partial Association Tree. *International Research Journal on Advanced Science Hub*, *3*(5), 6.

https://doi.org/10.47392/irjash.2021.137

Zhang, S., Chen, X., Ran, X., Li, Z., & Cao, W. (2024). Prioritizing Causation in Decision Trees: A Framework for Interpretable Modeling. *Engineering Applications of Artificial Intelligence*, *133*, 108224. https://doi.org/10.1016/j.engappai.2024.108224