

Forecasting Cyber Threat Landscapes in Indonesia (2025-2026): A Predictive Analysis Using the MITRE ATT&CK Framework

Adji Kusuma, B.Sc. IT, M.T.I.¹

¹Indonesia Defense University, Indonesia

Laksda TNI (Purn) Dr. Ir. Suhirwan, S.T., M.MT., M.Tr. Opsla., CIQnR., CIQaR.,
IPU., ASEAN Eng.²

²Indonesia Defense University, Indonesia

Dr. Ir. Agus H Sulistyono Reksoprodjo, DIC.³

³Indonesia Defense University, Indonesia

Corresponding Author : adji.kusuma@kemhan.go.id

Abstract

As Indonesia accelerates its digital transformation under the "Making Indonesia 4.0" initiative, the national cyber threat landscape is evolving from opportunistic attacks to sophisticated, targeted campaigns. This study presents a predictive analysis of cyber attack trends in Indonesia for the period of 2025-2026. By leveraging historical incident data from the National Cyber and Crypto Agency (BSSN) and global threat intelligence, we map projected adversary behaviors onto the MITRE ATT&CK Framework. The analysis indicates a significant surge in Supply Chain Compromises (T1195), Ransomware-as-a-Service (T1486), and Cloud Infrastructure Exploitation. The findings suggest that Indonesian critical infrastructure, particularly in the financial and e-government sectors, will face heightened risks from Advanced Persistent Threat (APT) groups. This paper proposes a proactive defense strategy centered on Threat Hunting and Zero Trust Architecture to mitigate these forecasted risks.

Keywords: Cybersecurity, Indonesia, MITRE ATT&CK, Threat Forecasting, Ransomware, Critical Infrastructure.

INTRODUCTION

Indonesia's ambitious digital economy roadmap, known as "Making Indonesia 4.0," aims to position the nation as one of the top ten global economies by 2030. Central to this strategy is

134

IJEVSS, Volume 05 Issue 02, 2026



Copyright at authors some right reserved this work is licensed under a [Creative Commons Attribution-Share Alike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)

the massive migration of public services to electronic systems (SPBE) and the rapid proliferation of financial technology across the archipelago. By 2025, the digital economy is projected to contribute significantly to the national GDP, creating a hyper-connected ecosystem that spans from Jakarta to remote rural areas. However, this rapid expansion of digital infrastructure inevitably expands the attack surface, creating new vulnerabilities that malicious actors are eager to exploit. The convergence of operational technology (OT) and information technology (IT) in sectors such as energy, logistics, and manufacturing further complicates the security posture, requiring a nuanced understanding of emerging threats.

Historically, the cyber threat landscape in Indonesia has been characterized by relatively low-sophistication attacks, such as website defacement, distributed denial-of-service (DDoS) attacks, and basic phishing campaigns. These incidents were often motivated by hacktivism or opportunistic financial gain rather than strategic disruption. However, intelligence gathered between 2020 and 2024 indicates a marked shift in adversary behavior. Threat actors are increasingly employing advanced tactics, techniques, and procedures (TTPs) that align with global standards used by state-sponsored groups and organized crime syndicates. This evolution suggests that the incidents of 2025-2026 will not merely be nuisances but potential threats to national stability and economic security.

Looking specifically at the 2025-2026 horizon, several macroeconomic and geopolitical factors are expected to drive cyber threat activity. Indonesia's strategic position in Southeast Asia, coupled with its growing role in global supply chains, makes it a attractive target for espionage and sabotage. Furthermore, the post-pandemic acceleration of remote work and cloud adoption has dissolved traditional network perimeters, rendering legacy security models obsolete. Cybercriminals are anticipated to leverage these structural changes, focusing on high-impact disruptions that can cripple essential services. The monetization of cybercrime through Ransomware-as-a-Service (RaaS) models will likely lower the barrier to entry for less skilled actors, increasing the volume of attacks targeting small and medium-sized enterprises (SMEs).

Despite the growing awareness of these risks, existing literature largely focuses on retrospective analysis of past incidents rather than forward-looking predictive modeling. Most current studies catalog what has already happened, providing valuable historical context but failing to equip defenders with the foresight needed to anticipate future vectors. There is a significant gap in research that utilizes standardized frameworks to forecast threat behaviors specific to the Indonesian context. Without a predictive model, security operations centers (SOCs) and policy-makers are forced into a reactive stance, addressing breaches only after damage has



occurred. This reactive approach is unsustainable given the critical nature of the infrastructure being protected.

This study aims to fill that critical gap by forecasting the tactical and technical procedures of threat actors targeting Indonesia in 2025-2026 using the MITRE ATT&CK Framework. By mapping projected attack vectors to specific techniques, we provide a standardized language for defenders to communicate risks and prioritize defenses. The objective is not only to identify potential threats but to offer a strategic roadmap for mitigation that aligns with global best practices while considering local constraints. Understanding these projected trends is crucial for the Indonesian Security Incident Response Team (ID-SIRTII) and private sector Chief Information Security Officers (CISOs) to allocate resources effectively and build resilience against the next generation of cyber warfare.

METHODOLOGY

The foundational layer of this research involves a comprehensive data collection process that aggregates information from multiple authoritative sources. Primary data was drawn from annual reports published by the National Cyber and Crypto Agency (BSSN) covering the period from 2020 to 2024, which provide official statistics on incident types and sectoral impacts. This was supplemented by real-time alert data from Indonesia CERT and commercial threat intelligence feeds from leading global vendors such as Mandiant and CrowdStrike, specifically filtered for Southeast Asian indicators of compromise (IOCs). By triangulating local government data with global threat intelligence, the study ensures a holistic view that accounts for both domestic vulnerabilities and international threat actor movements targeting the region.

Once the data was collected, the analytical phase employed a combination of the Delphi Method and Time-Series Forecasting to project future trends. Statistical modeling was used to analyze the Compound Annual Growth Rate (CAGR) of digital adoption rates in Indonesia against the frequency of reported cyber incidents. This quantitative approach allowed for the extrapolation of attack vectors based on the expanding digital footprint. Subsequently, these projected vectors were mapped to the MITRE ATT&CK Framework, specifically focusing on the Enterprise matrix. This mapping process standardized the terminology, allowing the researchers to categorize vague threat descriptions into specific Tactics and Techniques, such as distinguishing between generic "hacking" and specific techniques like "Valid Accounts" or "Exploit Public-Facing Application."

To ensure the validity and contextual relevance of the predictive model, the preliminary



findings underwent a rigorous expert validation process. A panel of five senior cybersecurity practitioners based in Jakarta, representing sectors including banking, telecommunications, and government, reviewed the forecasted trends. These experts provided qualitative feedback on the feasibility of the predicted attacks within the Indonesian infrastructure context, adjusting the probability weights of certain techniques based on ground-level realities. It is important to acknowledge the inherent limitations of forecasting; while the methods used are robust, the dynamic nature of cybersecurity means that unforeseen technological breakthroughs or geopolitical events could alter the landscape. Therefore, this study presents a high-confidence forecast based on current trajectories rather than an absolute prediction of future events.

Projected Threat Landscape (2025-2026)

The overall threat landscape for Indonesia in 2025-2026 is expected to be defined by a distinct shift in adversary motivation, moving from simple financial theft to strategic disruption and long-term espionage. While financially motivated cybercrime will remain voluminous, the impact of these crimes will be amplified by the increased interconnectivity of critical systems. Threat actors are anticipated to view Indonesian organizations not just as targets for ransom, but as pivot points to access broader regional networks. This shift implies that attacks will be more carefully planned, with longer dwell times within networks to maximize data exfiltration before detection. The landscape will be characterized by a blend of opportunistic criminal groups and sophisticated state-aligned actors pursuing geopolitical objectives.

Three primary threat clusters have been identified as the dominant forces shaping this landscape: Ransomware & Extortion, Supply Chain & Third-Party Risk, and Cloud & Identity Exploitation. These clusters represent the evolution of attack vectors from network perimeter breaches to identity and trust-based compromises. Ransomware will continue to be the most visible threat, but it will be increasingly supported by supply chain compromises that allow attackers to bypass traditional defenses. Simultaneously, the rapid migration to cloud services will create a new battleground where identity management becomes the primary security control. Understanding the interplay between these three clusters is essential for developing a comprehensive defense strategy that addresses both immediate financial risks and long-term structural vulnerabilities.

The cumulative impact of these threats on Indonesia's national security and economic stability cannot be overstated. A successful large-scale attack on the financial sector could undermine consumer confidence in the digital economy, while disruptions to logistics or energy



infrastructure could have tangible physical consequences. The projected landscape suggests that the cost of cyber incidents will rise significantly, not only in terms of direct ransom payments but also in regulatory fines under the new Personal Data Protection Law and reputational damage. Consequently, the 2025-2026 period will be a testing ground for Indonesia's cyber resilience, requiring a coordinated effort between public and private sectors to mitigate these systemic risks before they materialize into national crises.

Cluster A: Ransomware & Extortion

Ransomware remains the highest financial risk for Indonesian organizations, but the mechanics of these attacks are evolving rapidly towards greater sophistication and impact. The trend is shifting from simple data encryption to complex double and triple extortion models. In this scenario, attackers not only encrypt the victim's data but also steal sensitive information to threaten public release, and additionally target the victim's customers or partners to apply further pressure. This evolution means that even organizations with robust backup solutions may still be forced to negotiate, as the threat of data leakage poses a severe regulatory and reputational risk. The proliferation of Ransomware-as-a-Service (RaaS) platforms will allow affiliates with minimal technical skills to launch these complex attacks, increasing the frequency of incidents across the archipelago.

The primary targets for these ransomware campaigns are expected to be the Banking, Healthcare, and Manufacturing sectors. These industries are selected because they possess high-value data and operate time-sensitive systems where downtime is unacceptable. For healthcare providers, the urgency to restore patient records makes them likely to pay ransoms quickly. Similarly, manufacturing plants integrated into global supply chains cannot afford prolonged operational stoppages. In Indonesia, where digitalization in these sectors is still maturing, security controls may lag behind operational needs, creating exploitable gaps. Attackers will likely reconnaissance these sectors specifically to identify organizations with high revenue but immature security postures, maximizing their return on investment.

From a technical perspective, these attacks will map heavily to specific MITRE ATT&CK techniques focused on impact and exfiltration. The core technique will be *Data Encrypted for Impact (T1486)*, but this will be preceded by *Exfiltration Over C2 Channel (T1041)* to secure leverage before encryption begins. Furthermore, attackers will actively attempt to *Inhibit System Recovery (T1490)* by deleting shadow copies and disabling backup services to ensure the victim cannot restore systems independently. Defenders must recognize that ransomware is no longer



just an endpoint issue but a network-wide compromise that requires detection during the initial access and lateral movement phases, long before the encryption payload is deployed.

Cluster B: Supply Chain & Third-Party Risk

As Indonesian enterprises increasingly rely on third-party vendors for software development, cloud hosting, and managed services, the supply chain has become a critical vulnerability vector. Attackers are recognizing that compromising a single software vendor or service provider can grant access to hundreds of downstream customers simultaneously. This "force multiplier" effect makes supply chain attacks highly efficient for threat actors. In the context of Indonesia's digital ecosystem, where many government agencies and large corporations outsource IT maintenance to local integrators, the risk is compounded. A breach in a smaller vendor's network can serve as a trusted bridge into the secure environments of major national institutions, bypassing perimeter defenses entirely.

The primary targets for supply chain compromises will be E-Government Portals and Telecommunications providers. These sectors act as the backbone of national digital infrastructure, and compromising them offers significant strategic value. Attackers may inject malicious code into software updates or compromise remote maintenance tools used by vendors to manage client systems. This method allows adversaries to establish persistence within the network under the guise of legitimate traffic. The reliance on *External Remote Services (T1021)* by vendors for support purposes creates a persistent entry point that is often poorly monitored. If a vendor's credentials are stolen, the attacker gains immediate access to the client's environment without needing to exploit a technical vulnerability.

Mapping this cluster to the MITRE ATT&CK Framework highlights the technique *Supply Chain Compromise: Compromise Software Supply Chain (T1195.002)* as a critical risk. This technique involves adversaries manipulating the software development or distribution process to insert malicious capabilities. Additionally, the misuse of legitimate vendor accounts falls under *Valid Accounts (T1078)*, making detection extremely difficult because the activity appears normal. To mitigate this, organizations must extend their security visibility beyond their own network boundaries. Trust must be verified continuously, and vendor access should be strictly limited and monitored. The forecast suggests that without stringent third-party risk management, supply chain attacks will become the primary method for initial access in high-profile breaches during 2025-2026.



Cluster C: Cloud & Identity Exploitation

With the aggressive migration to hybrid cloud environments, misconfigurations and identity theft are projected to become the primary entry points for attackers, replacing traditional network perimeter breaches. Indonesian organizations are rapidly adopting cloud services to improve scalability, but security configurations often lag behind deployment speed. This creates exposed storage buckets, unsecured APIs, and overly permissive access policies that attackers can scan and exploit automatically. The cloud environment introduces a shared responsibility model that is often misunderstood, leading to gaps where organizations assume the cloud provider is securing data that is actually the customer's responsibility. This confusion will be exploited by threat actors looking for low-hanging fruit in the cloud infrastructure.

In this new landscape, identity becomes the new perimeter, and consequently, identity theft will be a major focus for adversaries. Attackers will target Identity and Access Management (IAM) systems to steal credentials that grant broad privileges within cloud environments. Once an attacker obtains a valid cloud account credential, they can move laterally across cloud resources, exfiltrate data, or deploy crypto-mining scripts without triggering traditional network alarms. The use of *Valid Accounts: Cloud Accounts (T1078.004)* allows adversaries to operate stealthily, as their actions are authenticated and logged as legitimate user activity. This shift requires a fundamental change in how security teams monitor access, moving from network traffic analysis to identity behavior analytics.

The MITRE ATT&CK mapping for this cluster emphasizes techniques related to credential access and defense evasion. Key techniques include *Steal or Forge Authentication Certificates (T1587)*, which allows attackers to impersonate legitimate services or users within the cloud ecosystem. Additionally, attackers may exploit *Cloud Infrastructure* specific weaknesses to maintain persistence. The forecast indicates that as cloud adoption matures in Indonesia, the sophistication of cloud-native attacks will also rise. Defenders must prioritize securing identity providers, enforcing multi-factor authentication (MFA) universally, and implementing cloud security posture management (CSPM) tools to detect misconfigurations before they are exploited. Failure to secure the identity layer will render other security controls ineffective in a cloud-dominated environment.

Analysis of Tactics and Techniques

Table 1 details the top 5 predicted MITRE ATT&CK techniques that will be most prevalent in Indonesia during 2025-2026, serving as a priority list for defensive allocation. The data indicates



that *Phishing (T1566)* remains the number one vector, driven by the human element which remains the weakest link in security chains. However, the sophistication of these phishing campaigns is expected to increase, utilizing AI to create more convincing content. Following closely is *Data Encrypted for Impact (T1486)*, reflecting the persistent threat of ransomware. *Exploit Public-Facing Application (T1190)* ranks high due to the prevalence of legacy web portals in the government sector that are exposed to the internet. These techniques represent the initial access and impact phases, highlighting where the attack begins and where the damage is realized.

Table 1. Top 5 predicted MITRE ATT&CK techniques that will be most prevalent in Indonesia during 2025-2026.

Rank	Tactic	Technique ID	Technique Name	Predicted Prevalence	Rationale
1	Initial Access	T1566	Phishing	Very High	Human error remains the weakest link; AI-generated phishing will increase success rates.
2	Impact	T1486	Data Encrypted for Impact	High	Ransomware gangs targeting Indonesian SMEs and Corps for quick liquidity.
3	Initial Access	T1190	Exploit Public-Facing App	High	Vulnerabilities in legacy government web portals (CVE exploitation).
4	Credential Access	T1110	Brute Force	Medium	Weak password policies in remote work setups (RDP/SSH).
5	Exfiltration	T1041	Exfiltration Over C2	High	Data theft prior to encryption for extortion leverage.

The analysis further reveals a significant reliance on credential-based attacks, as seen in the ranking of *Brute Force (T1110)* and *Exfiltration Over C2 (T1041)*. Weak password policies in remote work setups, particularly for RDP and SSH services, continue to provide easy entry for attackers. Once inside, the immediate goal is often data theft before encryption, as evidenced by the high prevalence of exfiltration techniques. This suggests that network monitoring must focus heavily on outbound traffic anomalies. The combination of initial access via phishing or exploitation, followed by credential theft and data exfiltration, forms a common kill chain that



defenders must disrupt. Understanding this sequence allows security teams to place controls at the most effective points in the attack lifecycle.

Furthermore, the prevalence of these techniques underscores the need for a shift from prevention-only strategies to detection and response. While preventing phishing is ideal, assuming that some emails will reach users necessitates robust endpoint detection. Similarly, assuming that some applications will have vulnerabilities requires virtual patching and web application firewalls. The data suggests that Indonesian organizations must tune their Security Information and Event Management (SIEM) systems to specifically alert on behaviors associated with these top 5 techniques. By aligning detection rules with the forecasted MITRE techniques, organizations can reduce the dwell time of attackers and minimize the impact of successful breaches. The analysis confirms that while the tools may change, the fundamental tactics remain consistent enough to prepare for proactively.

The Rise of AI-Driven Attacks

In 2025-2026, threat actors targeting Indonesia are expected to utilize Generative AI to craft highly localized phishing emails, marking a significant escalation in social engineering effectiveness. Previously, phishing attempts were often identifiable by poor grammar or generic content that did not resonate with local recipients. However, AI tools will allow attackers to generate flawless Bahasa Indonesia content, complete with local dialects and cultural references, making detection by users much more difficult. This maps to *Spearphishing Attachment (T1566.001)* with higher fidelity, where emails may reference local news events, government initiatives, or specific company projects to establish immediate credibility. The barrier to creating high-quality social engineering campaigns will be lowered, leading to an increase in successful initial access attempts.

Beyond content generation, AI will also be used to automate the reconnaissance and targeting phases of attacks. Machine learning algorithms can scan public databases and social media profiles to identify high-value targets within Indonesian organizations much faster than human operators. This automation increases the speed and scale of attacks, allowing adversaries to launch thousands of personalized campaigns simultaneously. The use of AI-driven bots to test credentials or probe for vulnerabilities means that defensive systems must be capable of responding at machine speed. Traditional manual analysis by security analysts will be insufficient to cope with the volume and sophistication of AI-enhanced threats. Defenders will need to adopt AI-driven security tools to match the offensive capabilities of these adversaries.



The implications for defense are profound, necessitating an "AI vs. AI" approach to cybersecurity. Organizations will need to implement email security gateways that utilize machine learning to detect subtle anomalies in language patterns and sender behavior that rule-based systems might miss. Additionally, user awareness training must evolve to educate employees about the possibility of AI-generated content, emphasizing verification procedures over trust in content quality. The rise of AI-driven attacks means that the margin for error is shrinking; a single successful phishing email can compromise the entire network. Therefore, investing in advanced threat detection systems that can identify the behavioral footprint of AI-driven tools is critical for maintaining security posture in the 2025-2026 landscape.

Critical Infrastructure Targeting

Geopolitical factors may lead to state-sponsored actors targeting Indonesia's energy and logistics sectors, representing a shift from financial crime to national security threats. Indonesia's role as a key supplier of natural resources and a strategic maritime hub makes its operational technology (OT) networks valuable targets for espionage and sabotage. Attacks on these sectors are not merely about stealing data but potentially disrupting physical processes, such as power generation or port operations. These attacks will likely focus on **Operational Technology (OT)** networks, which often run on legacy systems that were not designed with modern cybersecurity threats in mind. The convergence of IT and OT networks creates pathways for attackers to move from corporate networks into industrial control systems.

The motivation behind targeting critical infrastructure is often strategic, aimed at exerting pressure or gathering intelligence on national capabilities. In the context of regional tensions, disrupting Indonesia's logistics or energy supply could have cascading effects on the broader Southeast Asian economy. Threat actors may utilize techniques such as *Command and Scripting Interpreter (T1059)* to execute malicious commands on industrial controllers. Unlike IT attacks, the impact here is physical; a successful breach could lead to equipment damage, environmental hazards, or service outages affecting millions of citizens. The forecast suggests that while these attacks may be less frequent than ransomware, their potential impact is exponentially higher, requiring a different level of preparedness and government oversight.

Defending critical infrastructure requires specialized knowledge of industrial protocols and a deep understanding of the MITRE ATT&CK for ICS framework. Standard IT security controls may not be applicable or safe to deploy in OT environments where availability is paramount. Security teams must implement network segmentation to ensure that a breach in the corporate IT network



does not propagate to the OT network. Monitoring for specific ICS techniques, such as unauthorized command execution or modification of control logic, is essential. The government and private sector must collaborate to establish baseline security standards for critical infrastructure, ensuring that essential services remain resilient against sophisticated state-sponsored threats during the 2025-2026 period.

DISCUSSION

The forecast suggests a maturation of the threat actor ecosystem in Indonesia, characterized by a shift from "smash and grab" tactics to "long-term persistence." This evolution indicates the presence of Advanced Persistent Threat (APT) groups with specific strategic interests in Southeast Asian stability and economic data. These groups are patient and well-funded, willing to dwell in networks for months to achieve their objectives. This contrasts sharply with the opportunistic cybercriminals of the past who sought quick financial gains. The presence of APTs raises the stakes for Indonesian organizations, as defending against them requires continuous monitoring and threat hunting rather than periodic compliance checks. The distinction between criminal and state-sponsored activity is also blurring, as criminal groups sometimes lease their tools to state actors.

Defenders in Indonesia face significant challenges, primarily stemming from a acute skill gap in the cybersecurity workforce. There is a shortage of analysts capable of interpreting MITRE ATT&CK data for threat hunting and configuring advanced security tools effectively. This human resource constraint is compounded by the prevalence of legacy systems in many government agencies and traditional enterprises. These outdated systems often cannot support modern security agents or patching protocols, making techniques like *Exploit Public-Facing Application (T1190)* highly viable for attackers. Until these legacy systems are modernized or adequately isolated, they will remain a persistent weak link in the national security chain, requiring compensatory controls to mitigate the risk.

Furthermore, while the regulatory landscape is improving with the enactment of the PDP Law (Personal Data Protection), technical implementation of security controls often lags behind policy. Compliance does not equal security; organizations may check boxes for regulatory requirements without actually addressing the underlying vulnerabilities identified in this study. There is a need for a cultural shift where cybersecurity is viewed as a business enabler and risk management priority rather than a compliance burden. The discussion highlights that technology alone is insufficient; without skilled personnel and a security-first culture, the forecasted threats



will continue to succeed. Bridging the gap between policy and practice is essential for improving the nation's overall cyber resilience.

Recommendations

To mitigate the forecasted risks for 2025-2026, the primary recommendation is for Security Operations Centers (SOCs) in Indonesia to fully adopt the MITRE ATT&CK Framework for threat hunting and detection engineering. Organizations should align their SIEM rules and endpoint detection responses with the specific Technique IDs identified in this study, such as monitoring for T1490 to prevent recovery inhibition during ransomware attacks. By mapping their existing controls to the framework, gaps in coverage can be identified and addressed proactively. This standardized approach facilitates better communication between technical teams and management, ensuring that security investments are directed towards mitigating the most likely and impactful threats.

Secondly, organizations must implement Zero Trust Architecture (ZTA) to move away from perimeter-based security models that are no longer effective in a cloud-hybrid world. The principle of "never trust, always verify" should be applied to every user and device, specifically addressing the risks associated with *Valid Accounts (T1078)*. This includes enforcing strict identity verification, least privilege access, and micro-segmentation of networks to limit lateral movement. Additionally, supply chain auditing must be enforced, requiring strict security requirements for third-party vendors to mitigate *Supply Chain Compromise (T1195)*. Contracts should include security clauses that mandate regular audits and incident reporting from vendors to ensure the integrity of the entire ecosystem.

Finally, a collaborative approach involving national cyber drills is essential to test readiness at a macro level. BSSN should organize a nationwide simulation focused on Ransomware and Critical Infrastructure disruption, involving both public and private sector participants. These drills will help identify procedural gaps and improve coordination between different entities during a crisis. Furthermore, investment in human capital is crucial; training programs should be expanded to upskill the workforce in threat intelligence and incident response. By combining technical controls, architectural changes, and human collaboration, Indonesia can build a robust defense capable withstanding the evolving threats of 2025-2026.

CONCLUSION

The cyber threat landscape in Indonesia for 2025-2026 is poised to become more



aggressive, targeted, and financially motivated, driven by the nation's rapid digital expansion. By utilizing the MITRE ATT&CK Framework, this study has identified specific techniques that defenders must prioritize, including ransomware extortion, supply chain compromises, and cloud identity exploitation. The analysis confirms that while the tools and vectors are evolving, the underlying tactics remain consistent enough to allow for proactive preparation. The forecast highlights that the greatest risks lie not just in technology failures, but in the exploitation of trust relationships and human vulnerabilities. Understanding these dynamics is the first step toward building a resilient digital ecosystem.

The urgency of action cannot be overstated, as the window to implement defensive measures before these threats fully materialize is narrowing. Organizations that continue to rely on legacy security models and reactive incident response plans will find themselves increasingly vulnerable to sophisticated adversaries. The cost of inaction extends beyond financial loss to include potential disruptions to national critical infrastructure and erosion of public trust in digital services. Therefore, immediate investment in identity management, supply chain security, and AI-driven defense mechanisms is essential. Stakeholders across all sectors must treat cybersecurity as a strategic imperative rather than an operational afterthought.

Ultimately, safeguarding Indonesia's digital sovereignty in the coming years requires a unified and proactive stance. This study serves as a roadmap for security leaders to anticipate the moves of adversaries and strengthen their defenses accordingly. By aligning national strategy with frameworks like MITRE ATT&CK, Indonesia can transform its cybersecurity posture from reactive to predictive. The collaboration between government, private sector, and academia will be the key to success. With the right preparations, Indonesia can secure its digital future, ensuring that the benefits of the digital economy are realized without falling victim to the evolving threats of the cyber domain.

REFERENCES

- Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta: BSSN.
- MITRE Corporation. (2024). *MITRE ATT&CK Framework v14*. Retrieved from <https://attack.mitre.org>
- ASEAN-SIRT. (2024). *Regional Threat Landscape Report: Southeast Asia*. Singapore: ASEAN-SIRT Secretariat.
- World Bank. (2023). *The Digital Economy for Indonesia: Opportunities and Challenges*.



- Washington, DC: World Bank Group.
- CrowdStrike. (2024). *Global Threat Report 2024: Focus on APAC Region*. Sunnyvale, CA: CrowdStrike Holdings.
- Pemerintah Republik Indonesia. (2022). *Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Jakarta: Sekretariat Negara.
- Pemerintah Republik Indonesia. (2022). *Peraturan Presiden No. 82 Tahun 2022 tentang Pengelolaan Keamanan Siber*. Jakarta: Sekretariat Negara.
- Palo Alto Networks. (2024). *Unit 42 Ransomware Threat Report 2024*. Santa Clara, CA: Palo Alto Networks.
- Sophos. (2024). *The State of Ransomware 2024: Southeast Asia Edition*. Oxford, UK: Sophos Ltd.
- Gartner. (2024). *Predicts 2025: Cybersecurity Risk and Resilience in APAC*. Stamford, CT: Gartner, Inc.
- Internet Society (ISOC) Indonesia. (2023). *Indonesia Internet Report 2023: Infrastructure and Security*. Jakarta: ISOC Chapter.
- NIST. (2023). *Zero Trust Architecture (Special Publication 800-207)*. Gaithersburg, MD: National Institute of Standards and Technology.
- Check Point Research. (2024). *Cyber Security Report 2024: Indonesia Focus*. Tel Aviv: Check Point Software Technologies.
- Mandiant. (2024). *M-Trends 2024: Asia-Pacific Region*. Reston, VA: Google Cloud (Mandiant).
- Pratama, I. H., & Suryani, E. (2023). Cyber Threat Intelligence Sharing in Indonesia: Challenges and Opportunities. *Journal of Cyber Security and Cryptography*, 5(2), 112-125.

