International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1231-1242
Journal homepage: http://iieta.org/journals/ijsse

The Crucial Role of Red Teaming: Strengthening Indonesia's Cyber Defenses Through Cybersecurity Drill Tests

Semi Yulianto*, Benfano Soewito, Ford Lumban Gaol, Aditya Kurniawan

Computer Science Department, Doctor of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia

Corresponding Author Email: semi.yulianto@binus.ac.id

Copyright: ©2024 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.140420

Received: 10 May 2024
Revised: 29 July 2024
Accepted: 16 August 2024
Available online: 30 August 2024

Keywords:
cybersecurity, cybersecurity drill test, red teaming, regulatory compliance, Indonesia

ABSTRACT

This study delves into the critical role of red teaming in strengthening Indonesia's cybersecurity framework, with a particular emphasis on the heavily regulated banking and fintech sectors. The study aims to develop and assess advanced methodologies to improve organizational preparedness and compliance with stringent cybersecurity regulations amidst escalating cyber threats. Utilizing a mixed-methods approach, the study combines quantitative analysis of red team exercises with qualitative insights from industry experts. The findings indicate that red teaming is highly effective in identifying and mitigating security vulnerabilities, exposing hidden weaknesses that traditional assessments may overlook, and positively influencing regulatory compliance. The study highlights the strategic importance of red teaming as a core element of cybersecurity practices, offering valuable guidance for its implementation and impact on regulatory standards. By demonstrating the effectiveness of red teaming in fortifying cyber defenses and ensuring regulatory adherence, this study provides crucial insights for organizations and policymakers in enhancing Indonesia's overall cybersecurity strategy. The study emphasizes the essential role of red teaming in safeguarding sensitive financial data and maintaining the integrity of financial services in an increasingly complex digital threat landscape.

1. INTRODUCTION

In the era of Industry 4.0, Indonesia is experiencing a rapid digital transformation that brings both economic opportunities and significant cybersecurity challenges. The expansion of digital infrastructure has attracted sophisticated cyber threats, posing substantial risks to critical sectors, corporate domains, and government frameworks. In response, regulatory bodies such as the Ministry of Communication and Information Technology (KOMINFO), the Financial Services Authority (OJK), and the Central Bank of Indonesia (BI) have implemented stringent cybersecurity regulations. Despite these regulatory efforts, the dynamic nature of cyber threats necessitates advanced security measures beyond traditional approaches.

There is a pressing need to evaluate the effectiveness of current cybersecurity strategies within Indonesia's specific context, particularly in light of Industry 4.0 advancements. This evaluation is crucial to ensure Indonesian organizations can efficiently execute and optimize cybersecurity drill tests, notably red teaming, while adhering to sector-specific regulatory requirements. The research problem is to assess how well Indonesia's cybersecurity practices adapt to the challenges of Industry 4.0 and identify areas for improvement in strategy and implementation.

This study aims to address several key objectives. Firstly, it will assess the current cybersecurity practices in Indonesia, focusing on vulnerability assessments, penetration testing, and red teaming. Secondly, it will analyze Indonesian organizations' distinct regulatory and compliance challenges in implementing these security measures. Thirdly, the research will compare Indonesia's cybersecurity practices with global best practices to identify areas for enhancement and strategic initiatives. Furthermore, it will evaluate the impact of sector-specific threats and regulatory requirements on cybersecurity practices, particularly in critical sectors such as e-commerce, crypto-asset exchanges, and P2P lending. Lastly, the study will explore the selection process leading to red teaming and its effectiveness within Indonesia's regulatory framework.

The significance of this research is multi-faceted. It will inform policymakers, regulatory bodies, and organizations about the efficacy of current cybersecurity frameworks and potential areas for improvement. The findings will contribute to developing more robust and tailored cybersecurity strategies for Indonesia's digital landscape. Moreover, it will shed light on the unique challenges and opportunities in cybersecurity within an emerging economy embracing Industry 4.0. The study will help bridge the gap between regulatory requirements and practical implementation of advanced cybersecurity measures.

As Indonesia continues its digital transformation journey, developing and refining its cybersecurity strategies is crucial for ensuring a secure and prosperous digital future. This research aims to contribute to that goal by comprehensively

analyzing the current cybersecurity landscape and offering actionable insights for improvement. By addressing these research objectives, the study strives to guide future research endeavors in cybersecurity, especially in emerging economies grappling with the challenges of Industry 4.0 [1].

2. LITERATURE REVIEW

This section thoroughly analyzes the literature on Indonesia's cybersecurity challenges, regulatory frameworks, and the role of red teaming and cybersecurity drills in boosting organizational resilience. The review underscores the need for advanced defense strategies and continuous improvement in cybersecurity, especially in highly regulated sectors. It also highlights the importance of collaboration among government agencies, industry, and academia to strengthen Indonesia's overall cybersecurity posture.

2.1 Introduction to cybersecurity challenges in Indonesia

Cybersecurity challenges in Indonesia are multi-faceted and require a comprehensive approach to address. Several studies shed light on various aspects of cybersecurity in the Indonesian context. These studies highlight the critical issues faced by Indonesia in terms of cyberterrorism, cybersecurity policies, digital transformation, and the impact of cyber threats on different sectors.

Amrullah [2] emphasizes the issues and challenges posed by cyberterrorism in Indonesia, drawing attention to the need for robust cybersecurity measures. Intan and Intan [1] provide a case study reviewing cybersecurity policies and challenges in Indonesia, offering insights into the specific areas that require attention. Pratiwi et al. [3] delve into the analysis of cybersecurity challenges in Indonesia, focusing on threat identification and government responses.

Furthermore, Multazam and Widiarto [4] discusses the digitalization of the legal system in Indonesia, highlighting the importance of addressing challenges such as the digital divide, legal framework adaptation, and cybersecurity concerns. Dondokambey et al. [5] explores cybersecurity behavior in the banking industry, emphasizing the efforts of regulatory bodies to strengthen IT security systems and mitigate cyber risks.

Mahira et al. [6] stressed the need for an integrated cyber-resistance system in Indonesia to enhance national resilience against cyber threats. Margiansyah [7] points out Indonesia's vulnerability to cybercrime and cyberattacks, necessitating a robust cybersecurity strategy. Shiddique and Juned [8] underscores the importance of human capital development in cybersecurity to combat cyber threats effectively.

The studies collectively highlight the urgent need for Indonesia to bolster its cybersecurity measures across various sectors to mitigate cyber risks effectively. Addressing challenges such as cyberterrorism, policy frameworks, digital transformation, and human resource development is crucial to enhancing Indonesia's cybersecurity posture and safeguarding its digital infrastructure.

2.2 Regulatory frameworks and compliance in Indonesian cybersecurity

To explore the regulatory frameworks and compliance landscape in Indonesian cybersecurity, several studies offer valuable insights into the challenges, policies, and legal aspects shaping this domain.

Abrahams et al. [9] provide a comprehensive review of regulatory frameworks in accounting and cybersecurity, emphasizing the importance of mastering compliance in today's dynamic environment. Susila and Salim [10] conduct a comparative analysis of cyber espionage policies and regulations between Indonesia and Germany, highlighting the underdeveloped legal infrastructure for cybercrime in Indonesia. Isfihani et al. [11] examine the political law of electronic system implementation in Indonesia, focusing on data protection, cybersecurity, and the role of electronic systems in public administration.

Furthermore, Bakhtiyar et al. [12] discussed the juridical studies of the legal status of digital Rupiah in modernizing financial market infrastructure, emphasizing secure technology infrastructure, cloud-based cybersecurity services, and risk management systems. Ferdynandus et al. [13] emphasize implementing the NIST framework and the People, Process, and Technology approach in Indonesian financial services to counter evolving cybersecurity threats. Ramadhianto et al. [14] analyze presidential regulations concerning cybersecurity to bolster defense policy management, emphasizing cyber crisis management and national cybersecurity strategy.

These studies collectively highlight the importance of regulatory frameworks and compliance in Indonesian cybersecurity, underscoring the need for enhanced legal infrastructure, effective policies, and strategic management to address cyber threats and ensure data security.

2.3 Red teaming in cybersecurity: Fundamentals and methodologies

Red teaming in cybersecurity involves proactively identifying vulnerabilities and testing incident response capabilities through simulated adversarial attacks. Several studies provide valuable insights into the fundamentals and methodologies of red teaming in cybersecurity.

Chindrus and Caruntu [15] presents a case study on the red and blue cybersecurity competition, in which the Red Team assumes the role of the adversary to uncover vulnerabilities within the network. Vaishnavi et al. [16] emphasize the importance of red team exercises in Vulnerability Assessment and Penetration Testing (VAPT) for proactive cybersecurity by simulating cyber-attacks to enhance incident response capabilities.

Kotwani et al. [17] conduct a comparative analysis of red-teaming versus blue-teaming strategies in cybersecurity, highlighting how red-teaming identifies vulnerabilities and weaknesses through adversarial simulations. Metcalf and Singh [18] discusses the application of red-teaming strategies in governing large language models, drawing parallels with cybersecurity methodologies.

Yamin et al. [19] define red teaming as an information security assessment method that models cybersecurity adversaries to identify system vulnerabilities during exercises or tests. Alothman et al. [20] elaborate on the offensive role of the red team in launching cybersecurity attacks to test organizational defenses.

Red teaming is crucial in cybersecurity, as it proactively identifies weaknesses and enhances incident response capabilities. By simulating adversarial attacks, organizations

can strengthen their cybersecurity posture and mitigate risks effectively.

2.4 Effectiveness of red teaming in enhancing cyber defenses

To evaluate the effectiveness of red teaming in enhancing cyber defenses, it is crucial to consider insights from relevant studies in the field.

Chindrus and Caruntu [15] emphasize the importance of red teaming in securing networks through simulated adversarial competitions, enabling organizations to identify vulnerabilities and strengthen their digital defenses effectively. Oh et al. [21] introduce deep reinforcement learning in cyber-attack simulations to enhance overall cybersecurity defenses, stressing the significance of proactive measures in preparing for cyber threats.

Gutzwiller et al. [22] explores decision-making biases among professional red teamers in cyber-attack scenarios, suggesting that understanding these biases can benefit cyber defenders by reducing attacker interactions with network systems. Additionally, Alothman et al. [20] underscore the necessity to enhance cybersecurity defense due to the increasing and evolving nature of cyber threats, highlighting the role of red teaming in this context.

Moreover, Wang et al. [23] discussed a hybrid cyber defense mechanism that demonstrates improved defense effectiveness compared to single strategies, illustrating the positive impact of integrating different approaches in enhancing cybersecurity defenses. Sarjakivi et al. [24] investigate using wargaming to model cyber defense decision-making, offering insights into how blue teams can effectively plan and execute defensive cyber operations in realistic environments.

The effectiveness of red teaming in enhancing cyber defenses is evident through the proactive identification of vulnerabilities, simulation of adversarial attacks, and the continuous improvement of incident response capabilities. By leveraging red teaming methodologies, organizations can fortify their cybersecurity posture and better prepare for evolving cyber threats.

2.5 Red teaming in highly regulated industries

Red teaming in highly regulated industries presents unique challenges and opportunities that necessitate a tailored approach to cybersecurity. While the references provided do not directly address red teaming in highly regulated industries, insights from related studies can be synthesized to discuss this topic comprehensively.

Industries such as banking, healthcare, and pharmaceuticals are highly regulated, requiring stringent compliance with laws and standards [25]. In these sectors, the entry of Big Tech firms has raised concerns about data privacy and security [26]. The banking industry, for instance, faces information asymmetry challenges, necessitating robust cybersecurity measures [27].

Red teaming in highly regulated industries is crucial in identifying vulnerabilities and testing incident response capabilities while ensuring compliance with industry-specific regulations. The pharmaceutical industry, known for its stringent regulations, requires effective leadership to navigate compliance challenges [28]. Similarly, the healthcare sector benefits from red team exercises to enhance cybersecurity defenses and ensure regulatory compliance [26].

In highly regulated industries, the triadic relationship between customers, service providers, and the government influences compliance and cybersecurity practices [29]. Red teaming can help organizations in these sectors proactively assess risks, strengthen defenses, and align with regulatory requirements. By leveraging red team methodologies, companies can enhance their cybersecurity posture, mitigate risks, and ensure regulatory compliance in highly regulated environments.

Red teaming in highly regulated industries is essential for organizations to navigate complex regulatory landscapes, identify vulnerabilities, and enhance cybersecurity defenses effectively. By integrating red team exercises into their cybersecurity strategies, companies can proactively address threats, comply with regulations, and safeguard sensitive data in industries with stringent regulatory requirements.

2.6 Cybersecurity drill tests and red team exercises

Red teaming, also known as red team exercises and cybersecurity drill tests, are essential components of a robust cybersecurity strategy, playing a pivotal role in enhancing organizational cybersecurity defenses by simulating real-world cyber-attacks, identifying vulnerabilities, and testing incident response capabilities. Cybersecurity exercises, such as red teaming and drill tests, enable organizations to raise awareness, test capabilities, and identify strengths and weaknesses in their defense mechanisms [30]. Red team exercises specifically simulate cyber-attacks to identify vulnerabilities and enhance incident response capabilities proactively [24]. These exercises are crucial for organizations to stay ahead of evolving cyber threats and ensure preparedness.

Compliance with stringent laws and standards is paramount in highly regulated industries, making cybersecurity drill tests and red team exercises even more critical. By conducting continuous internal penetration testing and red team exercises, organizations can detect vulnerabilities, validate security controls, and ensure compliance with industry regulations [31]. Red teaming in highly regulated industries can help organizations navigate complex regulatory landscapes and strengthen their cybersecurity posture effectively.

Moreover, incorporating gamification approaches, such as red teaming and capture the flag challenges, can enhance cybersecurity training and simulation exercises, making learning activities more engaging and effective [32]. By integrating red teaming elements into cybersecurity exercises, organizations can provide participants with realistic scenarios to practice their skills and improve incident response capabilities.

Cybersecurity drill tests and red team exercises are crucial for organizations to proactively identify vulnerabilities, enhance incident response capabilities, and ensure compliance with industry regulations, ultimately strengthening their cybersecurity defenses.

2.7 Challenges and limitations of red teaming

Though an invaluable tool for enhancing cybersecurity defenses, red teaming has challenges and limitations. Understanding these aspects is vital for organizations to utilize red team exercises effectively. Based on the synthesized evidence, several key challenges and constraints of red

teaming have been identified.

One significant challenge is resource constraints. The availability of skilled red team members is often limited, making it difficult to find individuals with the expertise and knowledge necessary to simulate real-world cyber-attacks effectively [33].

Another challenge is the heavy reliance on human effort. Traditional red team exercises can be time-consuming and labor-intensive, hindering scalability and efficiency [34]. Their manual nature often limits their scope and impact.

There are also methodological challenges when it comes to AI red-teaming. Connecting AI red-teaming practices to address a wide range of AI harms can be complex. Ensuring these practices meet their objectives effectively requires careful consideration and planning [18].

Communication and trust issues can also arise, particularly in distributed teams. The lack of nonverbal communication and the difficulty in mastering advanced communication technologies can impact the effectiveness of red team exercises [35].

Compliance and regulation pose another significant challenge. Ensuring that red team exercises comply with industry-specific regulations and standards can be difficult in highly regulated industries. Organizations must navigate these regulatory requirements while conducting red teaming activities [36].

Another limitation is scalability. Scaling red team exercises to address evolving cyber threats and organizational needs is crucial. However, it can be challenging to ensure that these exercises remain effective and relevant as organizations grow and change [37].

Finally, incentivizing participation is essential for the success of red team exercises. Nevertheless, it can be difficult to maintain interest and encourage active engagement from all participants, including red team members, blue teams, and judges [38].

While red teaming is a valuable practice for bolstering cybersecurity defenses, organizations must be aware of the associated challenges and limitations. Addressing issues such as resource constraints, human effort, methodological challenges, communication difficulties, compliance concerns, scalability, and incentivizing participation is essential for maximizing the effectiveness of red teaming initiatives.

2.8 Impact of red teaming on organization culture and resilience

Red teaming, a practice that simulates adversarial attacks to identify vulnerabilities and test incident response capabilities, can significantly influence organizational culture and resilience. By analyzing various insights, we can explore how red teaming shapes these aspects within an organization.

Firstly, red team exercises can foster a positive organizational culture by encouraging diverse perspectives, promoting collaboration, and driving continuous improvement. According to Sun et al. [39], organizations that embrace disruption and growth opportunities through red-team strategies can cultivate a culture that values innovation, adaptability, and proactive risk management.

Secondly, red teaming enhances team cohesion and performance by encouraging teamwork, communication, and trust among members. Connell et al. [40] highlight that the collaborative nature of red team exercises can promote a sense of belonging and inclusiveness, which are crucial for maintaining a positive organizational culture.

Moreover, red teaming drives organizational learning and adaptability. AL Neyadi et al. [41] suggests that these exercises allow teams to reflect on their performance, learn from simulated attacks, and adjust their strategies accordingly. This continuous learning process enhances organizational resilience by enabling teams to respond effectively to evolving cyber threats and challenges.

Additionally, red teaming promotes psychological safety and innovation. Maan and Srivastava [42] argue that red team exercises create a safe environment where team members feel empowered to voice their opinions, share ideas, and experiment with new approaches. This culture of psychological safety fosters innovation, creativity, and a willingness to take calculated risks, which are essential for organizational resilience.

Finally, red teaming builds trust and accountability within teams and across the organization. Noch [43] notes that promoting transparency, accountability, and open communication through red team exercises can instill a culture of trust, integrity, and ethical behavior, further enhancing organizational resilience.

Red teaming can transform organizational culture and resilience by fostering collaboration, innovation, learning, trust, and adaptability. By integrating red teaming practices into their cybersecurity strategies, organizations can cultivate a culture that values continuous improvement, proactive risk management, and effective responses to cyber threats, ultimately strengthening their resilience against evolving challenges.

2.9 Future trends in red teaming and cybersecurity in Indonesia

As Indonesia continues to navigate the evolving cybersecurity landscape, future red teaming and cybersecurity trends are expected to shape the industry. We can anticipate key developments in this field by examining relevant references and extrapolating insights.

One significant trend is the increased adoption of AI and machine learning. The future of cybersecurity in Indonesia will likely see a growing reliance on artificial intelligence (AI) and machine learning for tasks such as threat detection, anomaly identification, and predictive analytics. Karunamurthy [44] states that AI-powered cybersecurity solutions can enhance threat detection capabilities and enable proactive defense mechanisms against sophisticated cyber threats.

Another important trend is a focus on cyber threat intelligence. Integrating AI and the Internet of Things (IoT) in critical sectors, such as power generation and distribution, is expected to drive the need for advanced cyber threat intelligence capabilities in Indonesia. Mohamed et al. [45] suggest that AI-driven analytics can help organizations anticipate, detect, and respond to cyber threats more effectively.

Enhanced resilience through red teaming is also anticipated to be crucial in Indonesia's cybersecurity future. Sarjakivi et al. [24] emphasizes that proactive red team exercises will be essential for identifying vulnerabilities, testing incident response capabilities, and strengthening cybersecurity defenses to mitigate risks effectively.

Collaboration is another emerging trend, with an increased emphasis on multidisciplinary approaches to address complex

cyber threats. Rane [46] highlights that the future of cybersecurity in Indonesia may involve more collaboration, effective communication, and cross-domain expertise, facilitating the development of innovative cybersecurity solutions and enhancing preparedness against emerging threats.

The adoption of advanced security technologies is also expected to rise. Technologies like threat intelligence platforms, endpoint detection and response (EDR) solutions, and security automation tools will likely become more prevalent in Indonesia. Benjamin et al. [47] note that these technologies can bolster cybersecurity defenses, streamline incident response, and improve security posture.

Lastly, there will likely be a strong emphasis on cybersecurity workforce development. Indonesia is expected to focus on workforce development initiatives to address the growing cybersecurity challenges, bridge the skills gap, and build a resilient cybersecurity workforce. Almoughem [48] suggests that training programs, certifications, and capacity-building efforts will be crucial in cultivating a skilled workforce capable of combating evolving threats.

The future trends in red teaming and cybersecurity in Indonesia are poised to embrace advanced technologies, collaboration, resilience-building practices, and workforce development initiatives to effectively mitigate cyber risks and safeguard critical infrastructure in the digital age.

2.10 Synthesis of findings

The studies reveal that cybersecurity challenges in Indonesia are complex and evolving. They encompass cyberterrorism, inadequate policy frameworks, digital transformation difficulties, and a critical need for human capital development. These challenges underscore the need for a robust and integrated cybersecurity strategy to effectively address vulnerabilities across various sectors and ensure comprehensive defense against emerging threats.

The studies also reveal that Indonesia's cybersecurity regulatory frameworks and compliance measures are underdeveloped, particularly in cyber espionage and data protection areas. The existing legal infrastructure lacks the robustness to tackle the growing cyber threats effectively. Strengthening these regulatory frameworks and enhancing compliance strategies are essential to safeguarding the country's sensitive data and critical infrastructure.

Red teaming is highlighted as a crucial proactive approach in cybersecurity. It plays a significant role in identifying system vulnerabilities and testing incident response capabilities through simulated adversarial attacks. The effectiveness of red team exercises lies in their ability to uncover weaknesses in an organization's defenses, which is vital for improving resilience and preparing for real-world cyber threats.

The effectiveness of red teaming in enhancing cyber defenses is further emphasized by its role in identifying vulnerabilities, improving decision-making processes, and fostering a culture of continuous improvement. These exercises provide organizations with valuable insights that help strengthen their cybersecurity posture and better prepare for evolving threats.

The studies suggest that several trends will shape the future of red teaming and cybersecurity in Indonesia. These trends include the increased adoption of advanced technologies like AI and machine learning, a stronger focus on cyber threat intelligence, and the importance of multidisciplinary collaboration. Additionally, there is a significant emphasis on cybersecurity workforce development to address the existing skills gap. These trends enable organizations to mitigate risks more effectively and safeguard critical infrastructure in an increasingly digital world.

However, the studies also identify significant gaps, particularly in the regulatory framework and the availability of skilled professionals. Addressing these gaps will be crucial for Indonesia to build a robust and resilient cybersecurity environment capable of responding to the challenges of the digital age.

3. METHODOLOGY

This section details the research design and methods used to examine the effectiveness of cybersecurity drills, focusing on red teaming in Indonesia's regulatory context. A mixed-methods approach, combining qualitative and quantitative techniques, was employed to understand how red teaming improves cybersecurity resilience and compliance. The section covers the selection of organizations, data collection methods, and analytical strategies, all aimed at capturing the complexities of cybersecurity in regulated industries. This methodology underpins the study's findings and offers valuable insights for practitioners and policymakers.

Figure 1 presents the comprehensive research methodology employed in this study, detailing the sequential phases of Research Design, Data Collection, and Analysis. The study adopts a mixed-methods design approach, integrating qualitative and quantitative research techniques and focusing on cybersecurity drill tests and red team exercises. This methodology thoroughly investigates the research problem by blending practical, hands-on testing with theoretical analysis.

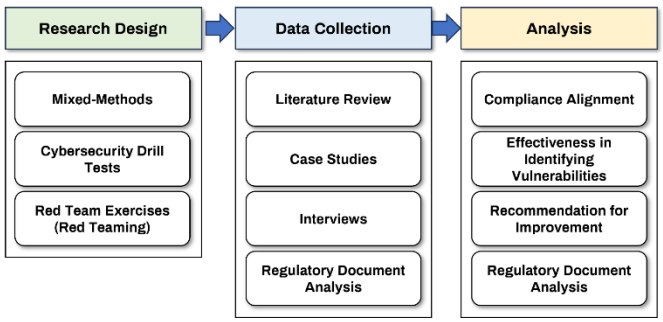

Figure 1. Research methodology

During the Data Collection phase, the study gathers diverse information through a systematic Literature Review, in-depth Case Studies, Expert Interviews, and thorough Regulatory Document Analysis. This multi-faceted approach ensures a holistic understanding of the current state of cybersecurity practices, particularly about red teaming.

The final Analysis phase evaluates the alignment of Red Teaming practices with compliance regulations and assesses their effectiveness in identifying security vulnerabilities. Based on this evaluation, the study provides targeted Recommendations for Improvement to enhance organizational cybersecurity defenses. The phase concludes with a further review of regulatory documents to ensure the proposed recommendations adhere to current legal standards. This structured process ensures a comprehensive investigation into

the application and impact of red teaming within the cybersecurity field, offering actionable insights for improving security practices.

3.1 Research design

The foundation of the research process begins with a well-thought-out design. By employing mixed methods, researchers are equipped to capture quantitative data, which provides measurable insights, and qualitative data, which offers a deeper understanding of the context and implications of cybersecurity issues. Including Cybersecurity Drill Tests and Red Team Exercises underscores this research design's practical, hands-on approach. These activities are theoretical and grounded in real-world scenarios where the organization's defenses are tested against simulated attacks. This combination of methods ensures that the research findings are robust, actionable, and directly applicable to enhancing cybersecurity strategies.

3.2 Data collection

The study employed mixed methods to investigate cybersecurity practices, focusing on red team exercises. These methods were strategically selected to comprehensively understand cybersecurity strategies' practical applications and measurable impacts within highly regulated sectors.

3.2.1 Qualitative approach

The qualitative aspect of the study began with a Literature Review, which served as a foundational step in the research process. This review was critical for building on existing knowledge in the field of cybersecurity and identifying gaps that the current study aimed to address. By grounding the research in established theories and findings, the literature review ensured that the survey was well-informed and contextually relevant.

Building on this foundation, the research included Case Studies that provided in-depth explorations of specific cybersecurity practices. These case studies allowed for a detailed examination of how red teaming and other security measures are applied in real-world scenarios, offering rich, contextual insights into the complexities and nuances of cybersecurity management.

To further enhance the practical relevance of the research, semi-structured interviews were conducted with fifteen (15) cybersecurity experts, mainly from financial services (e.g., banking, fintech, insurance). These interviews were meticulously designed with open-ended questions, enabling the researchers to delve into the participants' experiences, challenges, and perceptions regarding red team exercises. The participants were carefully selected based on their extensive experience with red teaming and significant roles in implementing cybersecurity protocols within their organizations. This method provided valuable, firsthand insights into the practical application of red teaming, its alignment with regulatory requirements, and its impact on organizational security culture.

A Regulatory Document Analysis was also performed to ensure the research aligned with the current regulatory environment. This analysis was crucial for integrating theoretical knowledge with practical applications, offering a holistic view of the cybersecurity landscape. The qualitative data collected from interviews underwent rigorous Thematic Analysis, a method well-suited for identifying and analyzing patterns within the data. Through this process, recurring themes and insights were uncovered, providing a coherent narrative that contributed to a deeper understanding of the role and effectiveness of red teaming in enhancing cybersecurity resilience.

3.2.2 Quantitative approach

The quantitative aspect of the research focused on data collected from Red-Teaming Exercises conducted within the participating organizations. These exercises involved simulated cyberattacks designed to test the organizations' defense and response capabilities rigorously. The data collected included key metrics such as the number of vulnerabilities identified, the time taken to detect and respond to attacks, the success rate of breach attempts, and the overall improvement in security posture following the exercises. These metrics objectively measured the organizations' cybersecurity performance under simulated attack conditions.

Descriptive statistics were employed to analyze the quantitative data, including calculating means and standard deviations, to summarize the findings effectively. This statistical approach allowed for a comprehensive assessment of the overall performance of the participating organizations, highlighting areas of strength and identifying statistically significant differences in the data. Furthermore, Correlation Analysis was conducted to explore the relationships between various variables, such as the impact of red-teaming exercises on detection and response times. This analysis provided deeper insights into the interconnectedness of different factors, enhancing the understanding of how red teaming contributes to cybersecurity resilience.

By integrating qualitative and quantitative data collection methods, the research offered a robust and multi-faceted examination of cybersecurity practices, particularly in red teaming. The qualitative methods provided rich, contextual insights and a deep understanding of the practical challenges and effectiveness of red teaming, while the quantitative methods offered measurable, objective data on its impact. Together, these approaches ensured that the research findings were comprehensive and actionable, contributing valuable knowledge to cybersecurity.

3.3 Analysis

The gathered data is systematically analyzed in the final stage to draw meaningful conclusions and provide actionable recommendations. Compliance Alignment is a key focus, ensuring that the organization's practices are effective and in line with industry standards and regulations. The effectiveness of identifying vulnerabilities is assessed to determine how well the organization can detect and respond to potential threats. This analysis is critical for identifying areas of weakness that need to be addressed. Based on these findings, the research offers Recommendations for Improvement to strengthen the organization's cybersecurity posture. The ongoing Regulatory Document Analysis ensures that these recommendations comply with legal requirements, providing a clear path forward for organizations looking to enhance their cybersecurity defenses.

3.4 Selection of target organizations for case studies

Three (3) organizations were carefully selected as case

studies for this study: an Indonesian e-commerce platform, a crypto-asset exchange platform, and a P2P lending company. These case studies provide a comprehensive overview of the cybersecurity landscape within Indonesia's digital economy, offering valuable insights into the intricate nature of cybersecurity challenges, responses, and regulatory compliance.

The rationale behind selecting these specific case studies is that they represent three critical sectors of the digital economy: e-commerce, cryptocurrency exchange, and peer-to-peer lending. This diversity provides a broad perspective on how different digital platforms approach cybersecurity, each facing unique threats and regulatory environments. The e-commerce platform represents the retail and consumer services sector, the crypto-asset exchange represents the financial technology and investment sector, and the P2P lending company represents the fintech lending space. Together, they cover a wide spectrum of the digital economy and offer insights into sector-specific and overarching cybersecurity challenges.

Each case study highlights different cybersecurity challenges, including social engineering and phishing attacks targeting human vulnerabilities and technical API security and encryption vulnerabilities. This variety underscores the complexity of cybersecurity in protecting both the technical infrastructure and human elements within organizations. By examining these diverse challenges, the selection illuminates the comprehensive nature of the threats faced by digital platforms and the necessity for multi-faceted security strategies.

Indonesia has a dynamic regulatory landscape for digital platforms, with specific guidelines and standards set by authorities such as OJK and BAPPEBTI. These case studies were chosen to demonstrate how different sectors navigate regulatory compliance while addressing cybersecurity threats. They provide valuable insights into how regulatory requirements influence cybersecurity practices and the strategic measures companies take to align with these regulations, highlighting the interplay between cybersecurity initiatives and regulatory adherence.

Each platform's response to identified vulnerabilities offers lessons in proactive and innovative cybersecurity practices. From enhancing cybersecurity training programs to implementing advanced encryption and machine learning algorithms, these case studies demonstrate a range of strategic responses that can inspire other organizations facing similar threats. The proactive measures and outcomes detailed in these case studies can serve as benchmarks for developing effective cybersecurity strategies.

Together, these case studies provide insights into each platform's specific challenges and responses and contribute to a deeper understanding of broader cybersecurity policy and practice implications in Indonesia. They offer valuable lessons for other organizations, regulators, and policymakers to enhance digital infrastructure security, foster a culture of cybersecurity awareness, and ensure agile adaptation of security measures in response to evolving threats and regulatory requirements.

These three case studies were selected because they offer a comprehensive outlook on cybersecurity challenges, strategies, and regulatory compliance in Indonesia's crucial digital economy sectors. Collectively, they illustrate the importance of tailored cybersecurity measures, the impact of regulatory frameworks, and the potential of innovative solutions to fortify the nation's cyber defense.

4. RESULTS

This section presents the study's findings, highlighting the outcomes of cybersecurity drills, especially the impact of red team exercises within Indonesia's regulatory framework. It analyzes how these exercises effectively identify vulnerabilities, strengthen defenses, and ensure regulatory compliance. The section also explores the challenges and successes in red teaming implementation, offering insights into how these strategies enhance organizational resilience against advanced cyber threats in Indonesia's regulated sectors.

4.1 Cybersecurity drill tests

This study examined various cybersecurity drills organizations utilize to accomplish specific security objectives and address multiple threats. These drills encompass automated simulations that actively search for vulnerabilities and provide prompt feedback, dynamic tabletop exercises that evaluate strategic response capabilities, physical security assessments to safeguard cyber assets, and social engineering drills to assess staff resilience against manipulative tactics. An essential component of this suite is red teaming, which employs an adversarial approach to rigorously challenge an organization's defenses through simulations of real-world cyberattacks. The inclusion of red teaming enhances the diversity of the drill tests and provides a critical perspective on the effectiveness of existing security measures. Collectively, these varied drill tests aid in identifying potential security weaknesses, assessing the efficacy of response strategies, and bolstering the overall vigilance of personnel, thereby comprehensively strengthening the organization's cybersecurity framework.

4.2 Red teaming findings

Red teaming plays a significant role in cybersecurity due to its effectiveness in simulating real-world attacks, allowing for identifying critical vulnerabilities. These exercises have proven to be essential in testing and demonstrating the resilience of security systems against complex threats. The main advantages of red teaming include increased threat awareness, improved readiness, and enhanced capabilities of security personnel, thanks to the realistic nature of attack scenarios. However, challenges remain in tailoring these simulations to match actual threat environments and conducting rigorous tests without disrupting day-to-day operations. In Indonesia, red teaming has emerged as a catalyst for regulatory changes, significantly strengthening the nation's cybersecurity strategies.

4.3 Compliance and improvement

Red teaming is essential in helping organizations meet and exceed the stringent cybersecurity standards of Indonesian regulations. As a specialized security audit, red team exercises allow organizations to test and refine their cybersecurity strategies rigorously. These exercises are designed to ensure that organizations are not only compliant with the stringent benchmarks set by Indonesian regulatory authorities but are also capable of responding effectively to increasingly sophisticated cyber threats. The insights gained from red team exercises have enabled organizations to navigate the complex and dynamic regulatory landscape, significantly enhancing their overall cybersecurity posture.

Moreover, by engaging in red teaming, organizations are proactively fortifying their defenses against cyber threats and fostering a culture of continuous improvement. This commitment to ongoing enhancement ensures compliance with existing regulations and prepares organizations to adapt to future regulatory changes and emerging threats. As a result, red teaming contributes to creating a more robust and secure digital environment across Indonesia, particularly in sectors that handle sensitive information, such as banking and fintech.

Cybersecurity drills are critical to organizational security protocols, meticulously designed to address various threats and objectives. These drills range from automated simulations that provide continuous monitoring and detection of vulnerabilities to tabletop exercises that allow for strategic planning and response to incidents. The strategic planning aspect of tabletop exercises is particularly beneficial, as it equips organizational leaders with the tools to respond effectively to potential incidents. They also include physical security assessments to protect cyber assets and social engineering drills to evaluate and enhance employee vigilance against deceptive tactics and potential breaches.

Among these various drills, red teaming stands out for its unique ability to simulate real-world attack scenarios. This technique is not just effective in identifying critical vulnerabilities and testing the resilience of systems against complex and sophisticated threats, but it also empowers cybersecurity teams. By subjecting systems to realistic and adversarial conditions, red teaming not only heightens threat awareness and preparedness but also hones the skills of cybersecurity teams through practical, hands-on experience. These teams gain invaluable insights into defending against actual attacks, making red teaming an indispensable tool in the ongoing effort to secure organizational assets.

However, the effectiveness of red teaming hinges on accurately calibrating these simulations to reflect the actual threat environment in which the organization operates. These exercises must be seamlessly integrated into normal business operations to avoid unnecessary disruption while still providing a rigorous test of the organization's cybersecurity defenses. Achieving this balance is key to maximizing the benefits of red teaming.

To illustrate the practical application of red teaming and other cybersecurity measures, Table 1 summarizes case studies involving three distinct Indonesian organizations: an e-commerce platform, a crypto-asset exchange platform, and a P2P lending company. The table outlines the cybersecurity challenges faced by each organization, the regulatory standards they aimed to meet, their strategic responses to identified vulnerabilities, the outcomes of their cybersecurity initiatives, and the key lessons learned from their experiences. This structured overview highlights the diversity of cybersecurity challenges across different sectors. It underscores the importance of a tailored approach to cybersecurity informed by red teaming and other proactive security measures. These case studies show how red teaming and a comprehensive cybersecurity strategy can significantly enhance an organization's resilience and compliance in Indonesia's evolving digital landscape.

The table's comparative analysis showcases the nuanced and industry-specific approach that organizations across various sectors in Indonesia adopt to enhance their cybersecurity defenses. Each case study highlights the significance of tailored cybersecurity initiatives in effectively addressing sector-specific risks and regulatory requirements.

To commence, the e-commerce platform's strategic focus on mitigating human vulnerability to phishing attacks reflects the prevalent cyber threats encountered in the online commerce sector. By aligning its cybersecurity efforts with industry-specific risks and compliance standards set by regulatory bodies such as the Financial Services Authority (OJK), the platform demonstrates a proactive approach to safeguarding customer data and maintaining trust in the digital marketplace.

In contrast, the crypto-asset exchange platform's emphasis on enhancing transaction systems and digital wallet security highlights the unique challenges inherent in cryptocurrency. With regulatory oversight from agencies such as the Commodity Futures Trading Regulatory Agency (BAPPEBTI), the platform navigates the complex landscape of crypto-asset exchanges by implementing advanced encryption protocols and robust authentication mechanisms to protect user accounts and digital assets.

Similarly, the strategic initiatives of P2P lending companies to fortify their online lending platforms against financial transaction-related cyber threats underscore the importance of safeguarding sensitive customer information and adhering to regulatory guidelines set by the Financial Services Authority (OJK). By implementing stringent security measures and adopting an agile cybersecurity framework, the company ensures continuous compliance with regulatory standards while enhancing user trust in the safety and integrity of their financial transactions.

Table 1. Comparative analysis of cybersecurity initiatives across diverse Indonesian industries

Aspect	E-Commerce	Crypto Asset Exchange	P2P Lending
Cybersecurity Challenge	Vulnerability to phishing attacks, highlighting deficiencies in staff's ability to recognize and counteract such attempts.	Vulnerabilities in API security and two-factor authentication processes, posing a risk of unauthorized access to user accounts and digital assets.	Critical vulnerabilities in the encryption of data transmissions and the fraud detection system, potentially allowing loan fraud.
Regulatory Compliance	Compliance with the Financial Services Authority (OJK) cybersecurity standards.	Compliance with regulations set by Indonesia's Commodity Futures Trading Regulatory Agency (BAPPEBTI).	Compliance with the Financial Services Authority (OJK) regulations, particularly data protection and financial transaction security.
Response	Conducted extensive cybersecurity drill tests, including social engineering drills; revamped cybersecurity training programs focusing on phishing techniques and preventive strategies.	Implemented advanced encryption for data in transit and at rest; strengthened two-factor authentication mechanisms; introduced continuous monitoring for anomalous activities.	Undertook red team exercises; enhanced encryption protocols; overhauled fraud detection system with machine learning algorithms; introduced rigorous access controls and authentication processes.

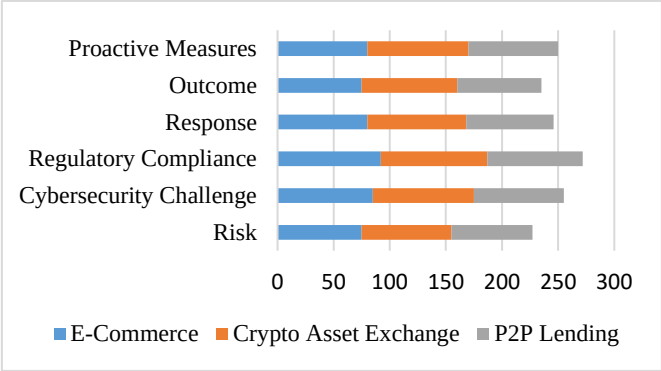

Figure 2. Statistical analysis of cybersecurity initiatives across diverse Indonesian industries

Figure 2 depicts a thorough statistical analysis of cybersecurity initiatives enacted across diverse industries in Indonesia. The study examines crucial facets, including cybersecurity challenges, regulatory compliance, response strategies, outcomes, proactive measures, and valuable insights from three distinct industry sectors. This offers a lucid and profound representation of the influence of cyber drill tests. The chart shows that the Crypto Asset Exchange sector leads in cybersecurity effectiveness, with high scores in regulatory compliance, response, outcomes, proactive measures, and learning from experiences. At the same time, the E-Commerce and P2P Lending sectors also perform well but have more room for improvement in certain areas.

Collectively, these case studies emphasize the critical role of tailored cybersecurity measures in mitigating industry-specific risks and regulatory obligations, thereby enhancing the overall resilience of Indonesia's digital ecosystem to the ever-evolving landscape of cyber threats. Organizations can effectively mitigate risks, protect sensitive data, and foster trust and confidence among stakeholders in the digital marketplace by aligning their cybersecurity strategies with sector-specific challenges and compliance requirements.

In the regulatory landscape of Indonesia, red teaming has emerged as a crucial tool, guiding organizations to meet and surpass the rigorous cybersecurity standards mandated by regulatory bodies. Red teaming provides organizations with invaluable insights as a comprehensive security audit, empowering them to strengthen their cybersecurity strategies and effectively navigate the intricate regulatory environment. The proactive embrace and ongoing refinement fostered by red teaming have played a significant role in bolstering the resilience of Indonesia's digital infrastructure.

5. CONCLUSION AND DISCUSSION

This study comprehensively examines the role of red teaming in enhancing cybersecurity within Indonesia's regulated industries, focusing on the banking and fintech sectors. Our research reveals that red teaming is critical for identifying vulnerabilities, improving regulatory compliance, and boosting organizational resilience against complex cyber threats. The findings of this study have significant implications for practitioners, policymakers, and researchers in the cybersecurity field, especially within Indonesia's rapidly evolving digital landscape.

5.1 The critical role of red teaming in Indonesian cybersecurity

Our analysis demonstrates that red teaming plays a pivotal role in three key areas:

- **Vulnerability identification:** Red team exercises prove exceptionally effective in uncovering hidden weaknesses in organizational cybersecurity defenses that traditional audits often overlook. In the Indonesian context, these exercises were particularly adept at identifying vulnerabilities related to legacy systems integration, a common issue in the country's rapidly digitalizing banking sector. They also exposed security gaps in mobile banking applications, which are gaining immense popularity in Indonesia but often lack robust security measures. Furthermore, red teaming revealed significant vulnerabilities in employee awareness and susceptibility to social engineering attacks, a critical factor given Indonesia's diverse workforce and varying levels of cybersecurity education.
- **Regulatory compliance enhancement**: Our study demonstrates that red teaming significantly improves compliance with Indonesia's evolving cybersecurity regulations. Specifically, it aids in meeting the requirements outlined in OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovation and Bank Indonesia Regulation No. 18/40/PBI/2016 on Payment Transaction Processing. Red team exercises provide concrete evidence of security measures' effectiveness, facilitating more comprehensive compliance reporting and helping organizations stay ahead of regulatory expectations in a rapidly changing digital environment.
- **Organizational resilience boosting:** By simulating advanced persistent threats (APTs) and nation-state-level attacks, red teaming prepares Indonesian organizations for high-level cyber threats. This is particularly crucial given Indonesia's geopolitical position and the increasing sophistication of cyber attacks targeting Southeast Asian financial institutions. Our findings indicate that organizations regularly conduct red team exercises, demonstrate markedly improved incident response times, and are better equipped to handle complex, multi-vector attacks.

5.2 Innovations and contributions of the study

This research makes several significant contributions to the field of cybersecurity, particularly in the Indonesian context:

- **Tailored red teaming framework:** We developed a comprehensive framework specifically designed for the Indonesian regulatory environment. This framework aligns red team objectives with Indonesia's unique cybersecurity challenges, such as the rapid adoption of digital banking in rural areas and the need for robust security in an increasingly mobile-first market. It incorporates cultural nuances that affect cybersecurity practices in Indonesian organizations, such as the tendency towards hierarchical decision-making structures and the importance of saving face. Additionally, our framework provides a structured approach to reporting red team findings that directly address regulatory requirements, facilitating clearer communication between security teams, management, and regulatory bodies.

- **Gap analysis and enhancement proposals:** Our research identified critical gaps between current red teaming practices and regulatory expectations in Indonesia. Key findings include a lack of emphasis on testing incident response capabilities, which are crucial in the Indonesian context due to the country's vulnerability to natural disasters and their potential impact on digital infrastructure. We also found insufficient focus on third-party risk assessment, a significant concern given the growing fintech ecosystem in Indonesia and the interconnectedness of financial services. To address these gaps, we propose incorporating disaster recovery scenarios into red team exercises, extending red team scope to include critical third-party providers, and developing a continuous feedback loop between red team findings and security strategy development. These enhancements not only align with but also surpass current regulatory standards, potentially driving the development of stronger cybersecurity regulations in Indonesia.
- **Advanced technology integration:** Our study pioneers the integration of artificial intelligence (AI) and machine learning into red team exercises within the Indonesian context. This innovation enables more sophisticated attack simulations that reflect the evolving threat landscape facing Indonesian financial institutions. It provides deeper insights into potential vulnerabilities in AI-driven financial services, which are gaining popularity in Indonesia. Moreover, this approach offers a forward-looking perspective on cybersecurity that aligns with Indonesia's Industry 4.0 aspirations, preparing organizations for future technological challenges.

5.3 Theoretical and practical implications

This study advances the theoretical understanding of red teaming by contextualizing it within Indonesia's unique cybersecurity landscape. It demonstrates how red teaming can be adapted to address the specific challenges emerging economies face with rapidly digitalizing financial sectors. Our research contributes to the broader literature on cybersecurity in developing nations, offering insights into how global best practices can be effectively localized.

Practically, our research provides actionable insights for various stakeholders:

- Financial institutions can use our framework to enhance their cybersecurity posture following Indonesian regulations and prepare for future threats.
- Regulators can leverage our findings to refine cybersecurity frameworks, ensuring they address evolving threats and technological advancements.
- Cybersecurity professionals can adapt our approach to tailor their red teaming practices to the unique characteristics of the Indonesian market.

5.4 Future research directions

Building on this study, we identify several promising avenues for future research:

- **Long-term impact assessment:** Investigate the long-term effects of regular red teaming on organizational security culture in Indonesian firms. This could involve longitudinal studies tracking changes in employee behavior, management attitudes, and overall security posture over time.
- **Cross-sector application:** Explore the effectiveness of cross-sector red team exercises in improving national cybersecurity resilience. This could involve collaborative exercises between financial institutions, government agencies, and critical infrastructure providers.
- **National framework development:** Examine the potential for establishing a national red teaming framework to standardize practices across industries in Indonesia. This could involve comparative studies with other nations that have implemented similar frameworks.
- **AI-enhanced threat modeling:** Further investigate the use of AI in predicting and simulating emerging cyber threats specific to the Indonesian context. This could lead to more proactive and adaptive cybersecurity strategies.
- **Regulatory impact analysis:** Conduct in-depth studies on how the implementation of red teaming practices influences the evolution of cybersecurity regulations in Indonesia. This could provide valuable insights for policymakers and regulators.

This study enhances the understanding and application of red teaming within Indonesia's regulated industries and lays a foundation for continued advancements in cybersecurity practices. By addressing Indonesia's unique challenges and opportunities in digital transformation, our research contributes significantly to strengthening the nation's cybersecurity posture in the face of evolving global threats. As Indonesia continues its journey towards becoming a major digital economy, the insights and methodologies presented in this study will play a crucial role in ensuring its cybersecurity capabilities keep pace with its digital ambitions.

REFERENCES

[1] Intan, A.A., Intan, R. (2023). Case study: A review of cybersecurity policies and challenges in Indonesia. In International Conference on Intelligent Computing & Optimization, Cham: Springer Nature Switzerland, pp. 266-273. https://doi.org/10.1007/978-3-031-50327-6_28

[2] Amrullah, K. (2024). Cyberterrorism and national security: Issues and challenges in contemporary Indonesia. Indonesian Journal of Counter Terrorism and National Security, 3(1). https://doi.org/10.15294/ijctns.v3i1.78905

[3] Pratiwi, F.I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D.Y., Dewi, C.S., Intan, A.A. (2024). Cybersecurity challenges in Indonesia: Threat and responses analysis. Perspectives on Global Development and Technology, 22(3-4): 239-264. https://doi.org/10.1163/15691497-12341660

[4] Multazam, M.T., Widiarto, A.E. (2023). Digitalization of the legal system: Opportunities and challenges for Indonesia. Rechtsidee, 11(2). https://doi.org/10.21070/jihr.v12i2.1014

[5] Dondokambey, V.A., Tambariki, C., Sondakh, O.B., Hendriana, E. (2023). Understanding cybersecurity behavior in the banking industry using protection motivation theory. Global Conference on Business and Social Sciences Proceeding, 15(1): 31-31. https://doi.org/10.35609/gcbssproceeding.2023.1(31)

[6] Mahira, D., Rohmahwatin, D., Suciningtyas, N. (2020). Strengthening multi-stakeholder integrated through shared responsibility in the face of cyber attacks threat. Lex Scientia Law Review, 4(1): 63-74.

https://doi.org/10.15294/lesrev.v4i1.38191
[7] Margiansyah, D. (2020). Revisiting Indonesia's economic diplomacy in the age of disruption: Towards digital economy and innovation diplomacy. Journal of ASEAN Studies, 8(1): 15. https://doi.org/10.21512/jas.v8i1.6433
[8] Shiddique, M., Juned, M. (2020). Human capital development for cybersecurity: Examining BSSN's contributions in the Indonesia-Australia cyber policy dialogue (2018-2020). Journal of Social and Political Sciences. https://doi.org/10.31219/osf.io/34rcb
[9] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O., Dawodu, S.O. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. Computer Science & IT Research Journal, 5(1): 120-140. https://doi.org/10.51594/csitrj.v5i1.709
[10] Susila, M.E., Salim, A.A. (2024). Cyber espionage policy and regulation: A comparative analysis of Indonesia and Germany. Padjadjaran Jurnal Ilmu Hukum (Journal of Law), 11(1): 122-144. https://doi.org/10.22304/pjih.v11n1.a6
[11] Isfihani, A.E., Izomiddin, Antasari, R.R., Is, M.S. (2024). Political law of electronic system implementation in Indonesia. Nurani Jurnal Kajian Syariah Dan Masyarakat, 24(1): 215-234. https://doi.org/10.19109/nurani.v24i1.22672
[12] Bakhtiyar, A.C., Rosadi, S.D., Handayani, T. (2023). Juridical studies of the legal status of digital rupiah in the context of modernizing financial market infrastructure. Jurnal Poros Hukum Padjadjaran, 5(1): 53-70. https://doi.org/10.23920/jphp.v5i1.1423
[13] Ferdynandus, F., Prihanto, J.N., Winarno, W. (2024). Implementing NIST framework and the people, process, technology approach in Indonesian financial services. International Journal of Engineering Continuity, 3(1): 172-182. https://doi.org/10.58291/ijec.v3i1.265
[14] Ramadhianto, R., Toruan, T.S.L., Kertopati, S.N.H., Almubaroq, H.Z. (2023). Analysis of presidential regulations concerning cyber security to bolster defense policy management. Defense and Security Studies, 4: 84-93. https://doi.org/10.37868/dss.v4.id244
[15] Chindrus, C., Caruntu, C.F. (2023). Securing the network: A red and blue cybersecurity competition case study. Information, 14(11): 587. https://doi.org/10.3390/info14110587
[16] Vaishnavi, S., Ananya, A.S., Akilesh, M.S. (2024). The importance of red team exercises in VAPT for proactive cybersecurity. International Journal of Advanced Research in Science Communication and Technology, 4(6): 639-644. https://doi.org/10.48175/ijarsct-17687
[17] Kotwani, B., Sawant, R., Chopra, S. (2023). Red teaming vs. blue teaming: A comparative analysis of cybersecurity strategies in the digital battlefield. International Journal of Scientific Research in Engineering and Management, 7(12): 1-11. https://doi.org/10.55041/ijsrem27675
[18] Metcalf, J., Singh, R. (2023). Scaling up mischief: red-teaming AI and distributing governance. Harvard Data Science Review, (Special Issue 5). https://doi.org/10.1162/99608f92.ff6335af
[19] Yamin, M., Katt, B., Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88: 101636. https://doi.org/10.1016/j.cose.2019.101636
[20] Alothman, B., Alhajraf, A., Alajmi, R., Farraj, R., Alshareef, N., Khan, M. (2022). Developing a cyber incident exercises model to educate security teams. Electronics, 11(10): 1575. https://doi.org/10.3390/electronics11101575
[21] Oh, S.H., Kim, J., Nah, J.H., Park, J. (2024). Employing deep reinforcement learning to cyber-attack simulation for enhancing cybersecurity. Electronics, 13(3): 555. https://doi.org/10.3390/electronics13030555
[22] Gutzwiller, R.S., Rheem, H., Ferguson-Walter, K.J., Lewis, C.M., Johnson, C.K., Major, M. (2023). Exploratory analysis of decision-making biases of professional red teamers in a cyber-attack dataset. Journal of Cognitive Engineering and Decision Making, 18(1): 37-51. https://doi.org/10.1177/15553434231217787
[23] Wang, S., Pei, Q., Zhang, Y., Liu, X., Tang, G. (2020). A hybrid cyber defense mechanism to mitigate the persistent scan and foothold attack. Security and Communication Networks, 2020: 1-15. https://doi.org/10.1155/2020/8882200
[24] Sarjakivi, P., Ihanus, J., Moilanen, P. (2024). Using wargaming to model cyber defense decision-making: Observation-based research in locked shields. European Conference on Cyber Warfare and Security, 23(1): 457-464. https://doi.org/10.34190/eccws.23.1.2270
[25] Mulyana, M., Syarief, R., Anggraeni, E. (2023). Business development strategy of PT XYZ as distributor LPG 3 kg in Cirebon. Jurnal Aplikasi Bisnis Dan Manajemen, 9(1): 94. https://doi.org/10.17358/jabm.9.1.94
[26] Özalp, H., Özcan, P., Dinçkol, D., Zachariadis, M., Gawer, A. (2022). Digital colonization of highly regulated industries: An analysis of big tech platforms' entry into health care and education. California Management Review, 64(4): 78-107. https://doi.org/10.1177/00081256221094307
[27] Hall, C.M., Hoffman, B.W., Liu, Z.H. (2020). Ownership structure and auditor selection. Managerial Auditing Journal, 35(8): 1121-1142. https://doi.org/10.1108/MAJ-07-2019-2360
[28] Mafaz, M.N.A., Abdullah, N.A. (2024). Transformational leadership on work performance in the pharmaceutical industry in Malaysia: An overview. Journal of World Science, 3(2): 258-270. https://doi.org/10.58344/jws.v3i2.550
[29] Quach, S., Thaichon, P., Hewege, C. (2020). Triadic relationship between customers, service providers, and government in a highly regulated industry. Journal of Retailing and Consumer Services, 55: 102148. https://doi.org/10.1016/j.jretconser.2020.102148
[30] Mäses, S., Maennel, K., Brilingaitė, A. (2022). Trends and challenges for balanced scoring in cybersecurity exercises: A case study on the example of locked shields. Frontiers in Education, 7: 1-13. https://doi.org/10.3389/feduc.2022.958405
[31] Alhammadi, M. (2023). Continuous internal penetration testing (CIPT). Authorea Preprints. https://doi.org/10.36227/techrxiv.23204669
[32] Kriesten, M., Thinyane, M., Ormrod, D. (2024). Leveraging gamification for cyber threat intelligence for resilience in satellite cyber supply chains. European Conference on Cyber Warfare and Security, 23(1): 716-723. https://doi.org/10.34190/eccws.23.1.2203

[33] Ferris, T., Camelia, F., Mattsson, T., Machado, R. (2022). Red-teaming as a research validation method for systems engineering thesis students. INCOSE International Symposium, 32(1): 529-544.
[34] Radharapu, B., Robinson, K., Aroyo, L., Lahoti, P. (2023). AART: AI-assisted red-teaming with diverse data generation for new LLM-powered applications. arXiv:2311.08592. https://doi.org/10.48550/arXiv.2311.08592
[35] Stray, V., Moe, N. (2020). Understanding coordination in global software engineering: A mixed-methods study on the use of meetings and slack. Journal of Systems and Software, 170: 110717. https://doi.org/10.1016/j.jss.2020.110717
[36] Capone, D., Caturano, F., Delicato, A., Perrone, G., Romano, S. (2022). Dockerized Android: A container-based platform to build mobile android scenarios for cyber ranges. arXiv:2205.09493. https://doi.org/10.48550/arXiv.2205.09493
[37] Behlendorf, B., Ackerman, G. (2022). DESSRT: A Novel framework for empirical red teaming at scale. Simulation & Gaming, 54(1): 5-27. https://doi.org/10.1177/10468781221093164.
[38] Tan, B., Karri, R., Limaye, N., et al. (2020). Benchmarking at the frontier of hardware security: Lessons from logic locking. arXiv:2006.06806. https://doi.org/10.48550/arxiv.2006.06806
[39] Sun, S.L., Zhang, Y.L., Zhu, Z. (2021). Turning disruption into growth opportunity: The red team strategy. Journal of Business Strategy, 43(6): 365-372.
[40] Connell, N., Zupanc, S., Lorenz, K., Bhatnagar, S., Fereydooni, S., Gamboa, R., Giannitrapani, K. (2023). Facilitators of palliative care quality improvement team cohesion. Health Care Management Review, 48(3): 219-228. https://doi.org/10.1097/HMR.0000000000000368
[41] AL Neyadi, S.N., Yaacob, T.Z., Hashim, H.I.C., Hasan, M.Z., Subramaniam, Y., Indiran, L. (2023). Cultivating virtual success: Exploring the influence of organizational culture on employee performance. International Journal of Academic Research in Business and Social Sciences, 13(12): 709-717. https://doi.org/10.6007/IJARBSS/v13-i12/19878
[42] Maan, P., Srivastava, D.K. (2023). Factors affecting team performance: An empirical study of Indian Gen Y and Gen Z cohorts. Equality Diversity and Inclusion an International Journal, 42(8): 986-1006. https://doi.org/10.1108/edi-05-2022-0114
[43] Noch, M.Y. (2024). The influence of leadership in audit teams on audit effectiveness. Golden Ratio of Auditing Research, 4(2): 56-65. https://doi.org/10.52970/grar.v4i2.390
[44] Karunamurthy, A. (2023). Human-in-the-loop intelligence: Advancing AI-centric cybersecurity for the future. Quing International Journal of Multidisciplinary Scientific Research and Development, 2(3): 20-43. https://doi.org/10.54368/qijmsrd.2.3.0011
[45] Mohamed, N., Oubelaid, A., Almazrouei, S. (2023). Staying ahead of threats: A review of AI and cyber security in power generation and distribution. International Journal of Electrical and Electronics Research, 11(1): 143-147. https://doi.org/10.37391/ijeer.110120
[46] Rane, N. (2023). Multidisciplinary collaboration: Key players in successful implementation of ChatGPT and similar generative artificial intelligence in manufacturing, finance, retail, transportation, and construction industry. https://doi.org/10.31219/osf.io/npm3d
[47] Benjamin, L.B., Adegbola, A.E., Amajuoyi, P., Adegbola, M.D., Adeusi, K.B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 19(2): 134-153. https://doi.org/10.30574/gjeta.2024.19.2.0084
[48] Almoughem, K. (2023). The future of cybersecurity workforce development. Academic Journal of Research and Scientific Publishing, 4(45): 37-48. https://doi.org/10.52132/ajrsp.en.2023.45.3