International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I6P140

Volume 73 Issue 6, 485-495, June 2025
© 2025 Seventh Sense Research Group®

Original Article

Threat Modeling and Cyber Risk Management for Mitigation of Attacks on Government XYZ Corporate Services Applications

Cakra Wibi Sasmito[1], Aditya Kurniawan[2]

[1,2]*Department of Computer Science, Bina Nusantara University, Indonesia.*

[2]*Corresponding Author : cakra.sasmito@binus.ac.id*

Received: 17 March 2025 Revised: 12 May 2025 Accepted: 10 June 2025 Published: 28 June 2025

Abstract - *This study aims to develop an end-to-end threat modelling and cyber threat remediation framework for the Corporate Services Application at Government XYZ. Since the cybersecurity threat landscape continues to evolve, government agencies need one threat modelling approach. This study fills the gap by integrating the NIST SP 800-30 risk management framework and MITRE ATT&CK, using threat intelligence from Web Application Firewall (WAF) and Intrusion Prevention System (IPS) logs. The suggested framework hierarchically decomposes, classifies, and prioritizes cyber threats to facilitate accurate risk estimation and mitigation plans specific to Government XYZ. According to the FAIR Institute's risk quantification model, impact analysis is also part of this study and is converted to Indonesian GDP to quantify financial loss due to cyber threats. By integrating these methods, organizations can develop a formal threat identification and risk assessment process, minimizing the intricacies of cybersecurity endeavors. The results can enable the identification of high-risk attack vectors, determine their economic effect, and inform the allocation of resources toward better security controls. The present study offers a practical guideline for government agencies to improve resiliency against cyber threats while supporting Indonesia's priority agenda for cybersecurity.*

Keywords - *Cyber risk management, Cybersecurity, MITRE ATT&CK framework, NIST SP800-30, Threat modeling.*

1. Introduction

Over the past few years, digital technologies have become increasingly prevalent in government operations worldwide, accelerated by the COVID-19 pandemic. In line with the global shift toward Industry 4.0, Indonesia has adopted ABCD technologies-Artificial Intelligence, Blockchain, Cloud Computing, and Big Data-to revolutionize the delivery of public services. Government XYZ, as one of the leading administrative departments in Indonesia, has been at the forefront of this transformation. In 2022, it launched the Corporate Services Application to span over 70,000 employees, with the core functions of internal communication, employee attendance, leave application, HR information, and performance evaluation. Delivered via a Single Sign-On (SSO) system, the application has improved operational efficiency while creating new challenges in cyber security. With more digital dependence comes more dangers. The average price of a data breach in the government sector was USD 2.6 million, based on IBM's Cost of a Data Breach Report 2023 [1]. The Global Risks Report 2024 of the World Economic Forum ranks cyberattacks in the top ten global risks [2]. In Indonesia, leaks of sensitive personal data were among the most potent cyber attacks in 2022, and cyber intrusions into governmental systems grew by 25% from 2021 [3]. Government XYZ detected over 12 million cyber threats aimed at its systems in 2023 alone, demonstrating the pressing necessity for a better, more organized cybersecurity defense [4]. In the wake of these threats, Government XYZ enacted Ministerial Decree No. 411/2023 on Information Security, Cybersecurity, and Personal Data Protection. The policy requires all digital assets to undergo formal threat modeling and cyber risk management, indicating the institution's desire to raise its cybersecurity posture. Recent research has explored various approaches to threat modeling in the public sector. The other significant work was conducted by Lani and Kurniawan [5], combining the MITRE ATT&CK framework and the NIST SP 800-30 risk assessment approach to improve cyber risk assessment in governmental agencies. They linked 13 adversary tactics and 475 techniques by analyzing vulnerability assessment reports and penetration testing. Although this is helpful information, such approaches are based chiefly on simulated attack exercises and static security testing that might not reflect adversary activity in real-time in operational environments. To address this shortcoming, the present study suggests a novel approach that leverages real attack telemetry from Intrusion Prevention System (IPS) and

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Web Application Firewall (WAF) logs. By mapping live data to the MITRE ATT&CK framework and threat prioritization through NIST SP 800-30 Rev.1, this article presents a more accurate, behavior-driven threat modeling process grounded in real-world adversary tactics and improves contextual cyber risk assessment.

The contributions of this research are:

- Presenting a live-data-based threat modeling methodology based on WAF and IPS logs;
- Showing the complementary efficacy of WAF and IPS for detecting various types of TTPs;
- Providing actionable recommendations for securing government digital assets;

Enabling compliance with Government XYZ's cybersecurity mandates. By integrating behavioral threat intelligence and structured risk analysis, this study presents an end-to-end proactive cyber risk management approach for governmental agencies in a constantly changing threat environment. We use the FAIR (Factor Analysis of Information Risk) model to estimate financial loss quantitatively as a secondary effect analysis. Merging the two provides a quantifiable perspective of risk exposure to augment qualitative estimations provided by MITRE ATT&CK and NIST SP800-30 Rev.1.

2. Related Works

Threat modeling and cyber risk analysis research have advanced quite a bit, primarily through the application of formal frameworks such as MITRE ATT&CK and NIST SP 800-30. These methods provide a structured mechanism for learning from adversaries' tactics and mitigating risk in governmental and sectoral contexts.

2.1. Analysis Based on Joint MITRE ATT&CK and NIST SP 800-30 Research

Lani and Kurniawan [5] incorporated MITRE ATT&CK and NIST SP 800-30 to improve cyber risk assessment in government agencies. They employed 13 tactics and 475 techniques used by adversary groups through vulnerability assessment, and penetration testing reports analysis. Ahmed et al. [6] performed the same integration in a healthcare organization, applying NIST 800-30's simulation-based methodology for mapping threats from hacker groups like Lazarus and menuPass. In Indonesia, Supristiowadi et al. [7] and Fikri et al. [8] integrated NIST SP 800-30 and ISO 27005 to enhance information security management for government and profit institution use.

2.2. MITRE ATT&CK Framework-Based Research Only

Xiong et al. [9] used the MITRE Enterprise ATT&CK Matrix for policy effectiveness improvement in the enterprise domain. Al Shaer et al. [10] suggested association rules in the context of ATT&CK to establish correlations between techniques to facilitate TTP prediction. Kwon et al. [11] introduced the Cyber Threat Dictionary tool, which combined MITRE ATT&CK with the NIST Cybersecurity Framework. Locally, Bokan et al. [12] used the ATT&CK framework for cybersecurity investment measurement in enterprise architecture.

2.3. NIST SP 800-30 and its Variants-Based Research

NIST SP 800-30 has been widely used for risk assessments in public and private sectors. Risks in E-Learning Edlink applications were compared by Putro et al. [16]. Aji et al. [17], Ain et al. [18], and Arifnur et al. [19] applied the framework for risk assessment of information systems in libraries, schools, and archives, respectively.

2.4. STRIDE and DREAD Research

STRIDE and DREAD remain popular for qualitative threat modeling. Faridi et al. [14] applied the models to model threats in Hospital Information Systems (SIMRS), and Laksono et al. [15] applied the same model in academic systems. These studies effectively determine threat types and quantify severity but lack behavioral attack mapping like MITRE ATT&CK.

2.5. General Reviews and Quantitative Frameworks

Xiong et al. [9] systematically reviewed cyber threat modeling literature, focusing on the evolution of techniques and tools. Ekstedt et al. [13] illustrated a quantitative direction by combining threat modeling and decision support capabilities. These works offer baseline insight to develop more data-driven and quantifiable cybersecurity methods further.

2.6. Research Contribution and Study Gap

Despite the increasing literature applying MITRE ATT&CK and NIST SP 800-30, much research is based on simulated exercises, qualitative research, or static analysis. Little research has leveraged live security telemetry—especially Web Application Firewall (WAF) and Intrusion Prevention System (IPS) logs—to generate real-time, behavior-based threat models. This study bridges this gap by proposing a combined approach that maps live WAF and IPS data to MITRE ATT&CK, prioritizes the threats using NIST SP 800-30 Rev.1, and quantifies loss impact using the FAIR framework in the context of the government sector in Indonesia.

3. Methodology

This research provides countermeasures to address the techniques and methods of cyber-attacks in the government sector, focusing on developing a cybersecurity risk management threat model in the Corporate Services Application of Government XYZ. The suggested concept merges the standards of NIST SP 800-30 Rev 1 Guide for Conducting Risk Assessments and the MITRE ATT&CK Based Analytics Development Method, which is likely to provide efficient suggestions for the problems occurring in the

application. The literature review is the starting point of the research, investigating similar literature, books, and existing research on the conditions of organizational assets to build a theoretical model. In the latter part, a suggested threat model and cyber risk management approach are formulated from findings and theories in the literature, and then asset mapping is done using MITRE ATT&CK. The third step is to collect and parse attack logs from the Intrusion Prevention System and Web Application Firewall with Python for analysis. Then, based on past analysis, a threat modeling and risk management framework are established. Finally, the study concludes with a summary of the proposed Threat Modeling and Risk Management suitable for the Government XYZ Corporate Services Application and suggestions for future research based on the findings established.

The proposed Threat Modeling and Risk Assessment Framework combines the guidelines of NIST SP 800-30 Rev 1 for risk evaluation with the MITRE ATT&CK Analytics Development Method to create a complete framework for information security risk management and analysis of potential threats. The combination allows for practical understanding, detection, and mitigation of security risks by combining two diverse frameworks. NIST SP 800-30 Rev 1 is centered on identifying, measuring, and managing information security risks, whereas the MITRE ATT&CK methodology is centered on attacker behavior analysis and attack patterns. The integrated methodology allows organizations to detect threats and behavior, categorize threat sources, rank security gaps, and create an integrated risk analysis founded on possible threats, attacker behavior, and attack impact.

3.1. Initial Condition Identification

Identification is carried out during this phase to obtain an overview of the Corporate Services Application process at the Government XYZ. The observations are made at the Information Systems and Technology Center, the Government XYZ. The observation aims to learn the operational procedures related to public application, such as the collection of Corporate Services Applications and corporate Services Application assets, and identify ongoing threats.

3.1.1. The Identification of Corporate Service Applications

This phase involves listing the applications that are the focus of this research for threat modeling and risk assessment. These include (a) the Front End for user interfaces used by Government employees to monitor internal applications, (b) Single Sign-On (SSO), an authentication mechanism allowing users to access multiple applications with a single set of credentials, and (c) the API Gateway, which manages, secures, and routes API traffic between users and backend services.

3.1.2. Identification of Corporate Services Application Assets

Based on the identification of the Corporate Services Applications above, the following is a table of ICT asset identification for the Corporate Services Applications at the Government XYZ:

Table 1. Corporate services asset

No	Domain	IP Address
1	abc.xyz.domain	xxx.xxx.xxx.xxx
2	def.xyz.domain	xxx.xxx.xxx.xxx
3	ghi.xyz.domain	xxx.xxx.xxx.xxx

3.1.3. Identification of Corporate Services Application Asset Topology

Following the asset identification process for the Corporate Services Application, the next step involves mapping the asset topology. This step is crucial to understanding the physical placement of critical components such as the Web Application Firewall (WAF) and Intrusion Prevention System (IPS) within the infrastructure.

3.1.4. Identification of Source Country and Source IPs of Attacks

After gathering information about the topology of Corporate Services Applications' assets, the next step is to identify attacks against those assets. This identification is based on an attack log in the Web Application Firewall (WAF) and Intrusion Prevention System (IPS) appliances. For example, WAF and IPS attack logs identified the top five countries with different IP Addresses that made the highest number of attacks, excluding Indonesia.

3.2. Identification of Threat Sources Based on Adversary Behavior or Groups

In this step, identifying threat sources based on adversary behaviour involves pinpointing potential attacker groups that could threaten organizations, particularly in the government sector. This process utilizes information from the MITRE ATT&CK framework. The steps for identifying threat sources include: first, specifying the industry of interest, focusing on attacker groups targeting the government sector; second, mapping relevant adversary groups using the MITRE ATT&CK database by searching for the keyword "Government"; and third, further refining the search by limiting it to active attacking groups based on categorization results. A summary of identified adversary groups is presented in a table detailing group IDs, names, suspected attacker locations, descriptions, and target locations.

3.3. The Classification of Threat Actor Groups Based on Tactics and Techniques

After identifying the attacker groups, the following process is classifying the threat sources based on their techniques and tactics. It involves mapping the groups against the MITRE ATT&CK framework using the ATT&CK Navigator tool. The procedure involves signing into the ATT&CK Navigator, selecting the desired matrix and layers, and searching for the threat groups based on the identified list. Every threat group receives a score of 1 for their techniques,

and the same is done for all groups. After layering all the threat groups, a new layer is formed from them, using score expressions specific to each group. The last layers are available for download in JSON and Excel formats for further analysis, e.g., the production of heatmaps indicating the most prevalent tactics and techniques employed by the detected threat groups. The output is presented in a table that gives an overview of the tactics, techniques, group names, and count of groups for each technique.

3.4. Web Application Firewall and Intrusion Prevention System Attack Logs Compared to MITRE ATT&CK Tactics and Techniques

The WAF and IPS attack logs are analyzed to find overlapped attack names targeting the Government XYZ Corporate Services Application. The exercise starts by collecting a comprehensive list of detected attacks from the WAF and IPS logs.

The attacks are then mapped to their respective tactics and techniques under the MITRE ATT&CK framework. Subsequently, the intersection between the two systems is examined to discern commonly utilized tactics and techniques by attackers. This analysis facilitates a comprehension of the attack strategies frequently implemented against the system.

3.5. Risk Identification, Analysis, and Assessment

This activity is crucial in threat modeling and cyber risk assessment, especially for the Government XYZ Corporate Services Application. It entails listing, examining, and prioritizing attacks according to their linked risks to mitigate high-risk threats efficiently. This evaluation considers vulnerabilities, frequency of attacks, and possible impacts, as highlighted in previous research.

3.5.1. Identification and Likelihood Analysis

Likelihood attack analysis is conducted by gathering attack information from the Intrusion Prevention System and Web Application Firewall logs, grouping them per tactic and technique, removing duplicates, and computing likelihood values from attack frequencies, then mapping to predefined likelihood ranges.

3.5.2. Identification and Analysis of Loss Impact

The impact analysis is based on the Cyber Risk Quantification (CRQ) methodology set out by the FAIR Institute using the Factor Analysis of Information Risk (FAIR) framework to estimate potential financial loss due to cyber-attacks by sector.

It measures the risk as detailed simulations, estimating loss exposure, event likelihood, and financial impact. Extrapolations were made using Gross Domestic Product (GDP) and population ratio-based scaling factors to adapt FAIR's United States-focused impact data to the Indonesian environment.

Calculating the Scaling Factors

Once the necessary data has been collected, the next step is to calculate the scaling factors based on GDP and Population:

$$\text{GDP Scaling Factor} = \frac{\textbf{GDP of Indonesia}}{\textbf{GDP of US}}$$

$$\text{Population Scaling Factor} = \frac{\textbf{Population of Indonesia}}{\textbf{Population of US}}$$

Computing the Combined Scaling Factor

The next step is to figure out the Combined Scaling Factor. Here is how it is calculated:

$$\text{Combined Scaling Factor} = \text{GDP Scaling Factor} \times \text{Population Scaling Factor}$$

Applying the Combined Scaling Factor to Financial Impact

Finally, the financial impact for Indonesia is estimated by applying the combined scaling factor to the U.S.-based loss estimates:

$$\text{Financial Impact (Indonesia)} = \text{Financial Impact (U.S.)} \times \text{Combined Scaling Factor}$$

This method guarantees a contextually apt estimation of cyber risk impact in Indonesia, adjusting for economic and population disparities between the two nations. The impact of loss is modified for various categories, such as ransomware, denial of service, and system intrusion. The methods are then mapped into particular categories based on FAIR principles to improve the estimation and analysis of the impact of loss in Indonesia.

3.5.3. Identification and Analysis of CVSS Values

As per the risk assessment process, the Common Vulnerability Scoring System (CVSS) serves as the de facto standard for quantifying vulnerability severity quantitatively and objectively. CVSS value calculation starts with comprehending each of the metrics under the Base Metrics, which are the key factors in vulnerability measurement that contribute to the overall risk factor. These metrics consist of parameters such as Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, and Availability, each with weights. Following determining these values, a mapping of techniques for the values of Base Metrics is performed to generate a general evaluation table. During the analysis stage, the CVSS base score is computed with the help of Impact and Exploitability formulas. The score is modified depending on whether the Scope parameter is changed. The outcome in a CVSS value for each technique enables systematic assessment and comparison between vulnerabilities.

3.5.4. Threat Modeling Based on Risk Values and Levels

In this final research stage, the focus shifts to quantifying cyber risks and classifying them into severity levels to support better decision-making and prioritization.

Calculating Risk Value

To estimate the level of risk, we use the following formula:

Risk Value = Likelihood × Impact × CVSS Score

Risk Level Calculation

Based on the risk value, levels are categorized as:

Table 2. Risk value and risk level

Risk Value	Risk Level
>200	High
101–200	Medium
0–100	Low

Through this process, organizations can gain clearer insights into how specific threat actors might attempt to launch attacks, helping them focus their mitigation efforts where they matter most.

4. Result and Discussion

4.1. Identification of Source Countries and IPs Conducting Attacks

This stage identifies three targeted assets-abc.xyz.domain**,** def.xyz.domain**,** and ghi.xyz.domain-by analyzing WAF and IPS logs.

Table 3. Example of findings source countries and IPs conducting attacks

Source Country	Source IP	Total Attacks
United Kingdom	xxx.xxx.xxx.xxx	499,185
Singapore	xxx.xxx.xxx.xxx	6,854
United States	xxx.xxx.xxx.xxx	2,209
Netherlands	xxx.xxx.xxx.xxx	1,315
Australia	xxx.xxx.xxx.xxx	832

The data collected from January to June 2024 was processed using Python to determine the top five source countries and unique IP addresses based on the number of attacks. The analysis was divided into three key components:

Source Country**,** Source IP, and Total Attacks**.** WAF and IPS logs were examined separately to ensure a more comprehensive threat discovery process. Below are examples of the findings:

4.2. Identification of Threat Sources Based on Adversary Behavior or Groups

This step identifies potential threat sources by examining attacker activities using the MITRE ATT&CK knowledge base.

The process involved searching for adversary groups on the MITRE ATT&CK website using the keyword' Government.'

The search revealed 47 attacker groups that have targeted government sectors in Asia. Below are five examples:"

Table 4. Attacker groups

Group ID	Group ID	Suspected Attacker Location	Suspected Target Location
G0138	Andariel	North Korea	Asia
G1007	Aoqin Dragon	China	Asia
G0050	APT32	Vietnam	Asia
G1002	BITTER	South Asian	Asia
G0142	Confucius	Unknown	Asia
…	…	…	…

4.3. Threat Group Classification Based on Tactics and Techniques

At this stage, tactics and techniques used by attacker groups are catagorized using the MITRE ATT&CK framework. Below are a few examples of findings:

Table 5. Tactics and techniques used by attacker groups

Technique ID	Technique Name	Groups Name	Number of Group
T1204.002	Malicious File	Aoqin Dragon, Andariel, MuddyWater, Magic Hound, WIRTE, …	20
T1566.001	Spearphishing Attachment	Tropic Trooper, Andariel, Confucius, MuddyWater, APT32, …	17
T1203	Exploitation for Client Execution	Tropic Trooper, Aoqin Dragon, Andariel, Confucius, MuddyWater, APT32, …	13
T1190	Exploit Public-Facing Application	MuddyWater, GALLIUM, Magic Hound, Earth Lusca, ToddyCat	5
T1068	Exploitation for Privilege Escalation	BITTER, APT32, Tonto Team, PLATINUM	4
…	…	…	..

4.4. Comparison Web Application Firewall and Intrusion Prevention System Attack Logs Using MITRE ATT&CK Framework

This study analyzes and visualizes attack logs from Web Application Firewalls (WAF) and Intrusion Prevention Systems (IPS) regarding tactics and techniques in the MITRE ATT&CK framework. WAF and IPS logs were compared, and rules filtered the attacks at the critical level. Analysis revealed that the abc.xyz.domain was under constant attack by Crawler (699), Known Exploits (1177), and WordPress Path Traversal (29). def.xyz.domain was attacked by Crawler (151), Known Exploits (625), and Dasan GPON Remote Code Execution (18), whereas ghi.xyz.domain was attacked by Crawler (369), Known Exploits (89), and OpenSSL Heartbleed Attack (27). These results illustrate the typical patterns of attacks on various assets, highlighting that good security practices should be enforced. The following MITRE ATT&CK tactics and techniques were matched for each attack based on keywords from attack definitions. It is valuable to note the overlap between WAF and IPS detections to determine shared tactics and techniques to enable more efficient mitigation mechanisms. By examining the interaction of security tools such as these, companies can discover complementary strengths and weaknesses in their defense layers.

The results show that WAF and IPS complement one another, detecting various but overlapping threats and that mapping detections to the MITRE ATT&CK framework gives further insight into redundancies and areas for improvement, ultimately strengthening threat detection and response capabilities. Significantly, T1068 (Exploitation for Privilege Escalation), T1203 (Exploitation for Client Execution), and T1190 (Exploit Public-Facing Application) were found to overlap between WAF and IPS logs, indicating key areas to be fortified for security controls and a broader strategy towards threat mitigation.

Table 6. Mapping of attack names to MITRE ATT& CK tactics and techniques

Attack Name	Tactic ID	Tactic Name	Technique ID	Technique Name
Crawler	TA0007	Discovery	T1046	Network Service Discovery
	TA0007	Discovery	T1083	File and Directory Discovery
Known Exploits	TA0004	Privilege Escalation	T1068	Exploitation for Privilege Escalation
	TA0001	Initial Access	T1190	Exploit Public-Facing Application
	TA0002	Execution	T1203	Exploitation for Client Execution
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	TA0002	Execution	T1203	Exploitation for Client Execution
	TA0004	Privilege Escalation	T1068	Exploitation for Privilege Escalation
OpenSSL.Heartbleed.Attack	TA0001	Initial Access	T1190	Exploit Public-Facing Application
	TA0007	Discovery	T1518	Software Discovery
…	…	…	…	...

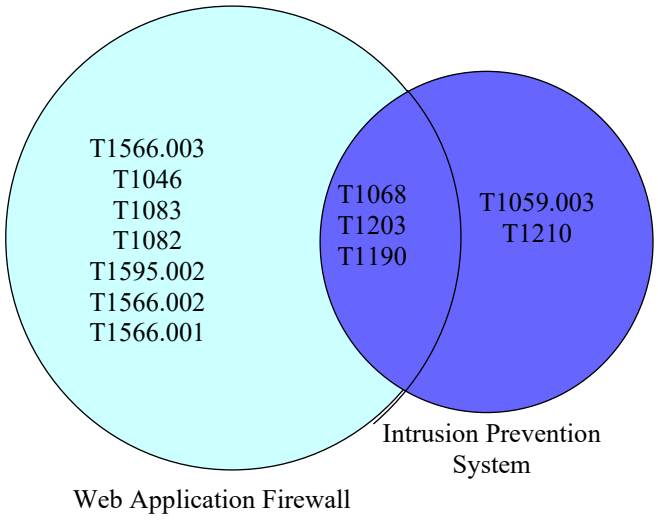

Fig. 1 Overlap techinque from WAF and IPS

4.5. Threat Modeling and Risk Levels

Threat modeling prioritizes risks by integrating probability/likelihood, loss impact, and CVSS scores. The attack names that appear for each asset are merged based on the attack list table, using data from Web Application Firewall (WAF) and Intrusion Prevention System (IPS) logs to identify and analyze the likelihood of attacks.

Then, the number of attacks is recorded in a table according to the corresponding tactics and techniques. Example of findings:

After calculating using the scaling factor formula, the less impact and its category based on the FAIR Institute are obtained, resulting in the following table:

Table 7. Aggregated attack counts per tactic and technique based on WAF & IPS logs

Tactic ID	Tactic Name	Technique ID	Technique Name	Number of Attacks
TA0007	Discovery	T1046	Network Service Discovery	2,664
TA0007	Discovery	T1083	File and Directory Discovery	2,664
TA0004	Privilege Escalation	T1068	Exploitation for Privilege Escalation	2,004
TA0001	Initial Access	T1190	Exploit Public-Facing Application	2,031
TA0002	Execution	T1203	Exploitation for Client Execution	1,980
…	…	…	…	…

Table 8. Categorization of MITRE ATT&CK tactics and techniques with associated loss impact values

Tactic ID	Tactic Name	Technique ID	Technique Name	Category (Based on FAIR Institute)	Value of Loss Impact
TA0007	Discovery	T1046	Network Service Discovery	System Intrusion	6
TA0007	Discovery	T1083	File and Directory Discovery	System Intrusion	6
TA0004	Privilege Escalation	T1068	Exploitation for Privilege Escalation	System Intrusion	6
TA0001	Initial Access	T1190	Exploit Public-Facing Application	Basic Web Attacks	5
TA0002	Execution	T1203	Exploitation for Client Execution	Basic Web Attacks	5
…	…	…	…	…	…

After completing all identifications-including the likelihood of attacks, impact assessment, and CVSS scoring-the next step is determining each technique's risk value and level. The results are in Table 9. The risk mapping is also visualized as a heatmap that illustrates the relationship between attack techniques and their corresponding risk values, as shown in Figure 2. From Table 9, the threat modelling is obtained in Figure 3.

4.6. Research Contribution

This study provides a meaningful contribution to developing cybersecurity practices within the government sector, particularly through an integrated approach that combines threat modelling and risk management based on real-world data.By merging the MITRE ATT&CK framework, the NIST SP 800-30 Rev.1 standard, and the FAIR quantitative model-adapted to Indonesia's economic context-this research offers a perspective that remains relatively underexplored in existing literature, especially with Indonesia's public sector. MITRE ATT&CK plays a crucial role in analyzing attack patterns found in Web Application Firewall (WAF) and Intrusion Prevention System (IPS) logs, mapping them to specific tactics and techniques commonly used by Advanced Persistent Threat (APT) groups. Once these techniques are identified, their risk levels are assessed using the NIST methodology, which considers the likelihood of occurrence, potential impact, and vulnerability severity (CVSS score).

In parallel, the FAIR model estimates financial losses in a localized economic context, considering indicators such as national GDP. Through this multidimensional approach, the study delivers a thorough technical analysis and actionable risk insights that are strategically relevant, empowering decision-makers and management teams to develop evidence-based cybersecurity strategies.

Table 9. Threat model and risk assessment

Threat Model				Risk Assessment						
Tactic ID	Tactic Name	Technique ID	Technique Name	Occurrence Count	Likelihood Score	Category (Based on FAIR Institute)	Loss Impact	CVSS Score	Risk Value	Risk Level
TA0007	Discovery	T1046	Network Service Discovery	2,664	9	System Intrusion	6	4,80	259,2	High
TA0007	Discovery	T1083	File and Directory Discovery	2,664	9	System Intrusion	6	2,00	108	Medium
TA0004	Privilege Escalation	T1068	Exploitation for Privilege Escalation	2,004	7	System Intrusion	6	8,41	353,22	High
TA0001	Initial Access	T1190	Exploit Public-Facing Application	2,031	7	Basic Web Attacks	5	4,85	169,75	Medium
TA0002	Execution	T1203	Exploitation for Client Execution	1,980	7	Basic Web Attacks	5	3,82	133,7	Medium
…	…	…	…	…	…	…	…	…	…	…

From Table 9., the threat modeling is obtained as follows in Figure 2.

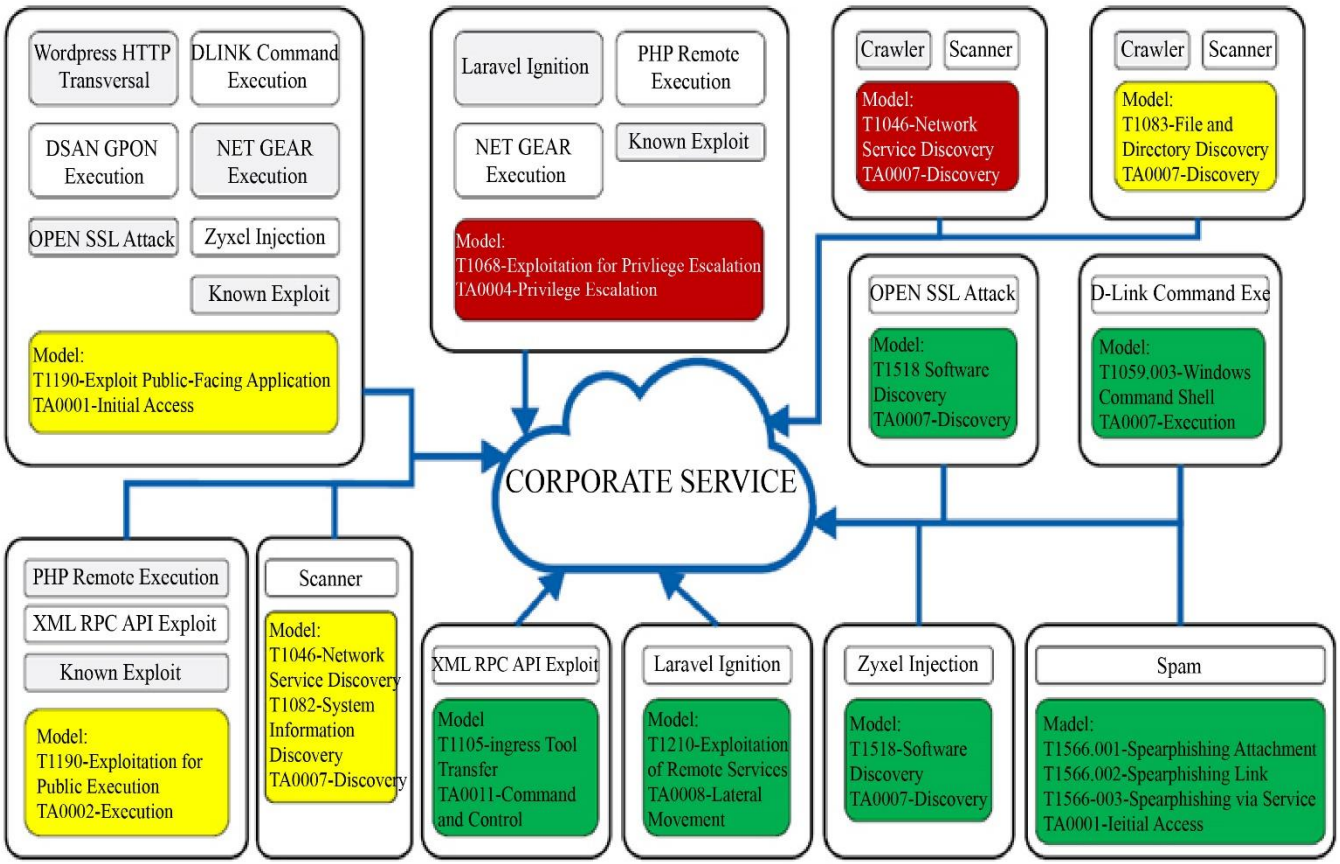

Fig. 2 Threat modeling with risk level

Fig. 3 Heatmap technique vs Risk value based on risk category

4.7. Reflection and Implication

Data collected from the XYZ Agency reveals that its three core digital assets, namely the Front-End Corporate Services, API Gateway, and Single Sign-On module, have been consistently targeted by cyberattacks, particularly through techniques such as T1068 (Privilege Escalation), T1190 (Exploit Public-Facing Application), and T1046 (Network Service Discovery). These attacks did not occur randomly but followed a systematic pattern involving reconnaissance, execution, and structured privilege escalation. The recurring presence of specific techniques across all assets suggests persistent vulnerabilities across multiple applications.

This pattern underscores a critical insight that the agency's current security posture remains largely reactive, relying heavily on perimeter-based defences with limited depth. The absence of internal threat detection mechanisms such as user behaviour monitoring and anomaly-based analytics exposes a significant gap in identifying and responding to more sophisticated or stealthy attacks. Additionally, the fact that many attacks occur during working hours highlights weaknesses in distinguishing legitimate user activity from disguised malicious behaviour.

The core implication of these findings is clear: the XYZ Agency must shift toward a threat-informed defence strategy that prioritizes real-world attacker techniques over theoretical assumptions. This approach empowers security teams to make data-driven decisions rooted in actual historical attack patterns within the organization rather than relying solely on external reports or generic industry benchmarks. As a result, the cybersecurity policies informed by this research would be far more contextual, adaptive, and operationally grounded—ultimately making the agency more resilient in the face of evolving digital threats.

This study carries practical implications for how information security is governed within Indonesian government institutions. First, the proposed threat-informed defence approach can serve as an operational standard to

support the implementation of Ministerial Decree XYZ No. 411 of 2023, particularly in developing digital asset threat models and designing realistic response scenarios. By embedding the MITRE ATT&CK framework into the modelling process, institutions like the XYZ Agency can ensure that threat mapping is grounded in actual attacker behavior rather than abstract assumptions.

Second, the findings provide a solid foundation for internal CSIRT teams to develop incident response playbooks based on specific techniques. Each identified tactic or technique can be linked to technical handling procedures, Indicators of Compromise (IoC), and targeted training policies. This enables faster response times and improves early detection capabilities—especially for critical systems vital to the agency's daily operations. Third, the framework designed in this research is both adaptable and replicable. Other agencies can use the same methodology to analyze their security logs, identify threats relevant to their context, and evaluate cyber risks using a data-driven approach. In doing so, this supports a more unified and standardized national readiness against cyber threats. Moreover, the locally contextualized FAIR model offers a way for government agencies to quantify cyber loss using economic measures that reflect national realities—allowing for better-informed security investment planning.

4.8. Future Works

This research has surfaced several intriguing findings that could serve as a springboard for future studies. One notable discovery is the recurring use of specific attack techniques linked to APT32 and APT41 identified through internal logs from the XYZ Agency. Although this study does not directly attribute the attacks to those groups, the strong alignment of techniques with those documented in the MITRE ATT&CK framework suggests that the agency may be a strategic target of nation-state adversaries. Future research could explore attribution more explicitly, examining the link between observed techniques and ongoing geopolitical cyber campaigns.

A key limitation of this study lies in its scope: the analysis focused on only three digital assets within a fixed observation window. Expanding future investigations to include additional systems and a longer monitoring period would help establish a more comprehensive and contextualized threat intelligence baseline. Furthermore, while the proposed mitigation strategies show promise, they have yet to be tested in a live production environment. Developing proof-of-concept implementations and conducting real-world testing would be essential to validate these strategies' technical and operational effectiveness.

From a policy standpoint, this research opens up opportunities for the XYZ Agency to build a more agile, threat-centric cybersecurity framework. Follow-up studies could contribute to shaping a formal roadmap for information security transformation, including creating early warning capabilities, strengthening CSIRT teams, and integrating mitigation strategies into the agency's strategic planning. These steps would improve the agency's cybersecurity posture and enhance national digital resilience in the long term.

5. Conclusion

This research successfully developed a threat model by integrating the MITRE ATT&CK framework and NIST SP 800-30 Rev. 1. By following steps such as identifying and analyzing the likelihood of attacks, assessing potential financial losses, and evaluating CVSS scores, the threat model and cyber risk management were effectively implemented. The key outputs of this integration include:

- Network Service Discovery (T1046) recorded the highest occurrence (2,664) with a high-risk level (259.2).
- Exploitation for Privilege Escalation (T1068) had the highest CVSS score (8.41) and a high-risk level (353.22), indicating a significant potential impact.

This research successfully developed a threat model by integrating the MITRE ATT&CK framework and NIST SP 800-30 Rev. 1. By following steps such as identifying and analyzing the likelihood of attacks, assessing potential financial losses, and evaluating CVSS scores, the threat model and cyber risk management were effectively implemented. The key outputs of this integration include:

- Network Service Discovery (T1046) recorded the highest occurrence (2,664) with a high-risk level (259.2).
- Exploitation for Privilege Escalation (T1068) had the highest CVSS score (8.41) and a high-risk level (353.22), indicating a significant potential impact.

This research successfully identified three attack techniques that overlap between Web Application Firewall (WAF) logs and Intrusion Prevention System (IPS) logs, namely:

- Exploitation for Privilege Escalation (T1068) with a CVSS score of 8.61, a risk score of 353.22, and a high-risk level.
- Exploitation for Client Execution (T1203) with a CVSS score of 3.82, a risk score of 133.7, and a medium-risk level.
- Exploitation of Public-Facing Application (T1190) with a CVSS score of 4.85, a risk score of 169.75, and a medium-risk level.

These techniques exhibit consistent attack patterns detected by both security devices and should be prioritized for mitigation efforts, focusing on patching vulnerabilities, securing public-facing applications, and protecting against malicious code execution.

Data Availability Statement

An anonymized version of the dataset used in this study-with all IP Addresses masked to protect confidentiality-is publicly available at: https://github.com/cakrawibi/anonymized-security-logs. The original data cannot be fully shared due to legal and ethical restrictions, as it contains sensitive Web Application Firewall (WAF) and Intrusion Prevention System (IPS) logs related to cyber-attack attempts.

Open Contributorship:

Cakra Wibi Sasmito: Conceptualization, Methodology, Data curation, Formal Analysis, Software, Investigation, Writing – original draft, Visualization. Aditya Kurniawan: Conceptualization, Resources, Supervision, Writing – review & editing.

References

[1] IBM Security, "*Cost of a Data Breach Report 2024*," IBM, 2024. [Publisher Link]

[2] "*The Global Risks Report 2024*," World Economic Forum, 2024. [Publisher Link]

[3] Positive Research 2023, Positive Technologies, 2023. [Online]. Available: https://global.ptsecurity.com/analytics/positive-research-2023

[4] Chuck Brooks, Cybersecurity Trends & Statistics For 2023; What You Need To Know, forbes, 2023. [Online]. Available: https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

[5] Mei Lanni, and Aditya Kurniawan, "Boosting Cyber Risk Assessment in Government Entities through Combined NIST and MITRE ATT&CK Threat Modeling," *Journal of System and Management Sciences*, vol. 14, no. 6, pp. 283-299, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mohamed Ahmed et al., "MITRE ATT&CK-Driven Cyber Risk Assessment," *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna, Austria, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Eko Supristiowadi, and Yudho Giri Sucahyo, "Information Security Risk Management in the Financial Application System at the Agency Level (sakti) of the Ministry of Finance," *Indonesian Treasury Review: Journal of Treasury, State Finance and Public Policy*, vol. 3, no. 1, pp. 22-33, 2018. [Google Scholar]

[8] Muhamad Al Fikri et al., "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique," *Procedia Computer Science*, vol. 161, pp. 1206-1215, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Xiong Wenjun, and Robert Lagerström, "Threat Modeling-A Systematic Literature Review," *Computers and Security*, vol. 84, pp. 53-69, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Rawan Al-Shaer, Jonathan M. Spring, and Eliana Christou, "Learning the Associations of MITRE ATT&CK," *2020 IEEE Conference on Communications and Network Security (CNS)*, Avignon, France, pp. 1-9, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Roger Kwon et al., "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," *2020 Resilience Week (RWS)*, Salt Lake City, UT, USA, pp. 106-112, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Branko Bokan, and Joost Santos "Threat Modeling for Enterprise Cybersecurity Architecture," *2022 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, USA, pp. 25-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mathias Ekstedt et al., "Yet another Cybersecurity Risk Assessment Framework," *International Journal of Information Security*, vol. 22, no. 6, pp. 1713-1729, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Muhammad Khairul Faridi, Imam Riadi, and Yudi Prayudi, "E-Health Security System Threat Modeling Using STRIDE and DREAD Methods," *Edumatic: Journal of Informatics Education*, vol. 5, no. 2, pp. 157-166, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Azis Catur Laksono, and Yudi Prayudi, "Threat Modeling Using STRIDE and DREAD Approaches to Identify Security Risks and Mitigation in Academic Information Systems," *JUSTINDO (Indonesian Journal of Information Systems and Technology)*, vol. 6, no. 1, pp. 9-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] A.A. Putro, A. Ambarwati, and E. Setiawan, "Edlink E-Learning Risk Management Analysis Using NIST SP 800-30 Revision 1 Method," *Journal of Technology and Information (JATI)*, vol. 11, no. 2, pp. 125-136, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ranggi Praharaningtyas Aji, Maruf Maftukhin, and Rizky Bangkit Bachtiar, "Information System Risk Management at Purwokerto Regional Library," *JATISI (Journal of Informatics Engineering and Information Systems)*, vol. 8, no. 1, pp. 261-272, 2021. [Google Scholar]

[18] Alma Iftina Azzahra Ain, Alawudiyah Ambarwati, and Lukman Junaedi, "Information Technology Risk Management and Asset Security Analysis Using Nist Sp 800-30 Revision 1," *Journal of Computer Science and Business*, vol. 13, no. 2a, pp. 155-165, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Adi Arga Arifnur, Hery Heryanto, and Yoga Megasyah, "Risk Management of Archiving Information Systems using NIST SP 800-30 at Kopertis Region IV Bandung," *The National Journal of Technology and Information Systems (TEKNOSI)*, vol. 9, no. 2, pp. 208-217, 2023. [CrossRef] [Google Scholar] [Publisher Link]