ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 14 (2024) No. 6, pp. 283-299
DOI:10.33168/JSMS.2024.0618

Boosting Cyber Risk Assessment in Government Entities through Combined NIST and MITRE ATT&CK Threat Modeling

Mei Lanni [1], Aditya Kurniawan [2]

[1]Master of Computer Science, Bina Nusantara University,
[2]Computer Science Department, School of Computer Science, Bina Nusantara University
Jakarta 11480, Indonesia

mei.lanni@binus.ac.id, aditya.kurniawan@binus.ac.id

Abstract. This study is driven by the imperative to cultivate a comprehensive framework for identifying and mitigating cyber threats within government organizations, a critical need in the ever-evolving cybersecurity landscape. This research addresses a conspicuous research gap by developing an integrated threat modeling approach that marries the NIST SP 800-30 and MITRE ATT&CK frameworks, offering a transformative path toward enhanced cyber risk management for government entities. The research problem lies in the absence of a systematic methodology for prioritizing and mitigating cyber threats within government environments. This gap is especially prominent in the Asian context, where a coherent framework for dealing with these threats is urgently required. To rectify this situation, our study introduces an innovative approach that harmonizes the well-structured risk assessment processes outlined in NIST SP 800-30 with the MITRE ATT&CK-based analytic development method. NIST SP 800-30 provides a meticulous framework covering threat analysis, vulnerability assessment, probability analysis, impact determination, and control analysis—a systematic guide for identifying and evaluating potential risks encountered by organizations. In parallel, the MITRE ATT&CK-based analytic development method enables in-depth exploration of potential attacks by referencing adversary techniques. This empowers organizations to proactively uncover potential threats and craft precise mitigation strategies. Our research's primary goal is to bridge this critical gap by leveraging the MITRE ATT&CK framework to analyze and categorize threats, thereby streamlining cybersecurity strategies. By merging these two approaches, organizations can utilize NIST SP 800-30's structured framework to establish a consistent risk assessment structure while deploying the MITRE ATT&CK-based method for detailed threat analysis and precise mitigation strategy development. This synergy amplifies organizations' capability to holistically and effectively combat information security threats. By identifying frequently used techniques with high-risk scores, organizations can optimally allocate resources, bolster security measures, and strategically channel cybersecurity efforts where they are most essential. This research serves as a practical blueprint for enhancing government organizations' resilience and detection capabilities in the face of ever-evolving cyber threats

Keywords: Cybersecurity, Risk Assessment, NIST SP 800-30, MITRE ATT&CK, Threat Modeling, Cyber Threats, Government Organizations, Asian Region.

1. Introduction

In the continuously evolving digital era, the role of the government sector in providing public services and maintaining the functions of the state has become increasingly crucial. However, with the growing reliance on information technology and communication, the government sector has also become more vulnerable to cyber threats. According to a report on Indonesia's cybersecurity landscape released by the National Cyber and Cryptography Agency in 2022 (*Cybersecurity in Indonesia 2022*, 2022), Indonesia faces serious challenges in managing cybersecurity. The staggering numbers are evident in the volume of anomalous traffic, which reached 976,429,996. Furthermore, attention is drawn to the government administration sector, considered the most vulnerable to cyberattacks, as noted in the report on cyber complaint services, recording 236 complaints in 2022. This reflects significant concerns from various stakeholders involved. To address these challenges, the sector's categorization based on Presidential Regulation No. 82 of 2022 regarding the Protection of Vital Information Infrastructure (VII) becomes highly relevant. To achieve optimal cybersecurity, a structured and targeted approach is required. The concept of threat modeling plays a significant role. Threat modeling is a systematic process for identifying, classifying, and evaluating potential threats to information systems (Adam Shostack, 2014). It involves a deep analysis of how attackers might attempt to exploit existing vulnerabilities. This approach can assist organizations in understanding the workings of attackers, detecting system weaknesses, and developing smarter mitigation strategies.

The purpose of this research is to assist government organizations in confronting the complexity and depth of cyber threats in a more systematic and structured manner. This is achieved by integrating two proven effective approaches in managing cybersecurity risks:

1. **MITRE ATT&CK**: MITRE ATT&CK is a globally accessible knowledge source that describes the tactics, techniques, and procedures used by attackers in cyberattacks. This approach helps organizations understand how attackers operate and provides insights into the tactics that may be employed in an attack.(Nickels, n.d.)
2. **NIST SP 800-30 Rev.1**: The NIST framework provides robust guidance for conducting cybersecurity risk assessments. It aids organizations in identifying and managing risks through a systematic approach.(NIST, 2012)

This research will combine these two frameworks to create a comprehensive approach to cybersecurity risk management. The primary objectives of this research are as follows:

1. **Threat Identification:** Through the integration of NIST and MITRE ATT&CK, this research will assist government organizations in identifying various tactics, techniques, and procedures that attackers may use in cyberattacks.
2. **Accurate Risk Assessment:** With a deeper understanding of threats, this research will help organizations conduct more accurate risk assessments, enabling them to assess the probability and impact of potential attacks.
3. **Mitigation Strategy Development:** This research will provide guidance on how government organizations can develop effective mitigation strategies based on the identified threats.
4. **Implementation Demonstration:** An essential aspect of this research is the practical demonstration of the integrated threat modeling approach in the context of cybersecurity risk management for government organizations.

Thus, the aim of this research is to address the gap in cybersecurity risk management by providing a stronger and more effective approach to protecting critical assets and data for the continued operational success of government organizations in the face of increasingly complex and pervasive cyber threats.

2. Related Works

Threat modeling and risk modeling are essential processes in information security to identify potential threats, vulnerabilities, and risks to an organization's systems and assets. This literature review aims to explore the use of MITRE ATT&CK and NIST SP 800-30 Rev 1 frameworks in threat and risk modeling.

MITRE ATT&CK-driven Cyber Risk Assessment

Assessing the risk posed by Advanced Cyber Threats (APTs) presents significant challenges when lacking an understanding of the methods and tactics employed by adversaries targeting an organization. MITRE ATT&CK provides valuable insights into the motivations, capabilities, interests, and the tactics, techniques, and procedures (TTPs) employed by threat actors. This paper harnesses these insights to facilitate informed characterization and assessment of cyber risks. Specifically, the paper leverages the MITRE repository of known adversarial TTPs, in conjunction with attack graphs, to ascertain both the probability and the likelihood of success of a cyberattack. Additionally, it identifies attack paths with the highest potential for success, taking into account the techniques and procedures utilized by threat actors. The assessment is illustrated through a case study involving a healthcare organization, which evaluates the level of risk posed by two adversary groups—Lazarus and menuPass. In essence, this research paper demonstrates how the MITRE ATT&CK framework can be employed as a powerful tool to enhance cyber risk assessment by delving into threat actors' behaviors and tactics, ultimately contributing to more informed decision-making and improved cybersecurity strategies. (Ahmed et al., n.d.)

Threat Modeling in Smart Firefighting Systems: Aligning MITRE ATT&CK Matrix and NIST Security Controls

This paper introduces a threat modeling framework for smart cyber-physical systems (CPS) to gain insight into potential security risks. The study focuses on the smart firefighting use case, based on the MITRE ATT&CK matrix. The matrix analysis provides a structured approach for detecting and mitigating attacks, while the System Requirement Collection (SRC) gathers generic asset information related to hardware, software, and network components. Utilizing the SRC and MITRE ATT&CK, a threat list specific to the smart firefighting system is generated. In conclusion, the generated threat list is mapped to the National Institute of Standards and Technology (NIST) security and privacy controls. The results indicate that these mapped controls can be effectively employed to protect and mitigate threats in smart firefighting systems. In the future, critical cyber-physical systems can adopt use case-specific threat modeling, leveraging the presented framework for enhanced security. (Zahid et al., 2023)

Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping.

This paper discusses the evolving challenges in operational technology (OT) security in line with the increasing connectivity of smart systems. The "big data boom" phenomenon in Internet of Things (IoT) devices, coupled with the vulnerabilities of unmonitored security, has raised concerns about the security of critical infrastructure facilities. In this journal, a crucial tool called the "Kamus Ancaman Siber" (Cyber Threat Dictionary/CTD) is introduced to address these challenges. CTD utilizes the mapping of the MITRE ATT&CK Matrix into the NIST Cybersecurity Framework, providing practical solutions and responses to cyber threats. This framework assists facility operators in identifying gaps, designing efficient mitigation strategies, connecting cyber attack techniques with control measures, prioritizing vulnerabilities, and devising preventive solutions. By enhancing incident response plans and aligning with NIST CSF, CTD empowers owners of critical infrastructure to strengthen the security of their facilities amid evolving threats. (Kwon et al., 2020) This research provides an overview of how the utilization of Matrix mapping, particularly in the context of government organizations, can serve as a global knowledge source that describes the tactics, techniques, and procedures used by attackers in cyberattacks. This mapping aims to gain a deeper understanding of various attacker groups and how

they operate within the context of government organizations.

A Review of Threat Modeling approaches for APT-Style attacks
aims to establish the boundaries of Threat Modeling and focuses on identifying approaches that can be used to model APT-style attacks. The findings of this research suggest an attacker-centric and asset-centric approach as the foundation for Threat Modeling research with an Attacker-centric approach. (Tatam et al., 2021)

Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix
aims to develop Threat Modeling based on the MITRE Enterprise ATT&CK Matrix. The results support security configuration analysis and architectural changes. (Xiong et al., 2022)

Relationship-Based Threat Modeling
The paper introduces relationship-based threat modeling (RBTM), which allows for the systematic and automatic generation of a threat graph using explicitly captured threat relationship knowledge. RBTM eliminates the need for manual consideration of threat relationships during risk assessments and enables stakeholders to clearly identify and communicate the rationale behind resulting risk values.(Verreydt et al., 2022)

Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis
This book presents the Process for Attack Simulation & Threat Analysis (PASTA) threat modeling methodology. It focuses on applying security countermeasures commensurate with the possible impact sustained from defined threat models, vulnerabilities, weaknesses, and attack patterns. The book discusses integrating threat modeling within different types of Software Development Lifecycles (SDLCs) and emphasizes threat modeling and risk management.(Ucedavélez & Morana, 2015)

Threat Modeling Tools: A Taxonomy
This paper proposes a taxonomy of threat modeling tools to understand the conceptual differences between them. While not specifically focusing on MITRE ATT&CK and NIST SP 800-30 Rev 1, the taxonomy provides a framework for comparing and categorizing various threat modeling tools.(Shi et al., 2022)

Modeling Features Threats to the Security of Information in the Process Threat Hunting
The article analyzes techniques and approaches for modeling information security threats, including proactive search for threats and the use of the MITRE ATT&CK framework. It also discusses the possibility of integrating the methodology of the Federal Service for Technical and Export Control of Russia (FSTEC of Russia) and MITRE ATT&CK for a more practice-oriented approach to modeling information security threats. (Ponomareva et al., 2023)

Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment
This paper presents a quantitative, integrated threat modeling approach that merges software and attack-centric techniques. It describes a threat model composed of a system model and component model, leveraging Common Vulnerability Scoring System (CVSS) for quantifying vulnerabilities. The case study focuses on a railway communication network. (Potteiger et al., 2016)

Privacy Risk Assessment for Data Subject-Aware Threat Modeling
This paper addresses the mismatch between privacy risk notions in threat modeling and regulatory efforts like GDPR. It proposes a data subject-aware privacy risk assessment model to support privacy threat modeling activities. The model allows for a more holistic understanding of privacy risk and proposes improvements to privacy threat modeling, such as enriching Data Flow Diagram (DFD) system models with appropriate risk inputs. (Sion et al., 2019)

In conclusion, the literature review highlights various approaches and methodologies for threat and risk modeling using MITRE ATT&CK and NIST SP 800-30 Rev 1 frameworks. These frameworks

provide valuable resources for identifying threats, assessing risks, and developing effective risk mitigation strategies. Organizations can leverage these frameworks to enhance their understanding of potential threats and improve their overall security posture.

3. Methodology

This research provides a solution to the issues of potential cyber attack tactics and techniques that may arise in the government sector, and how steps can be taken to develop a threat model for cyber risk management within an organization. The proposed idea in this study is the integration of recommendations from NIST SP 800-30 Rev 1 for Guide for Conducting Risk Assessments with the MITRE ATT&CK Based Analytics Development Method. It is expected to offer recommendations for the challenges that emerge within the organization.

In general, a qualitative research method with a common flow is used, as shown in figure 1.

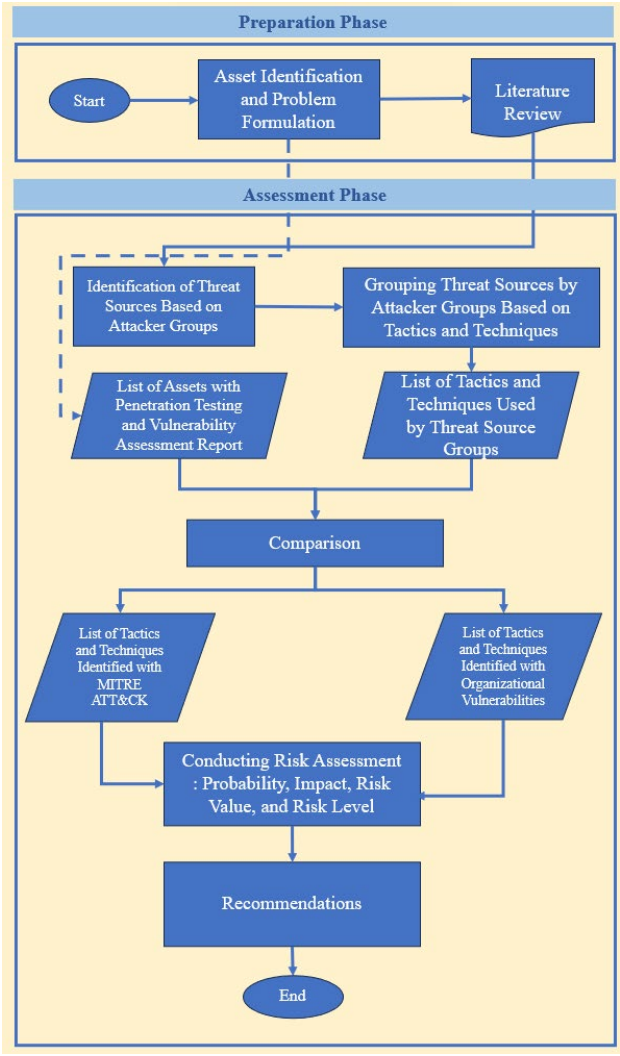

Fig.1: common flow

Here are the steps of the common flow:

a. Preparation Phase
   1. Start
      The first step is to initiate the risk assessment process.
   2. Asset Identification and Problem Formulation

Identify the assets to be assessed for risk and formulate the problems to be addressed.

3. Literature Review
   Conduct a literature review to gain a deeper understanding of the issues and appropriate solutions for the risk assessment

b. Assessment Phase

1. Identification of Threat Sources Based on Attacker Groups
   Identify the attacker groups involved in attacks on government organizations.
2. Grouping Threat Sources by Attacker Groups Based on Tactics and Techniques
   Classify threat sources based on the tactics and techniques used by the identified attacker groups.
3. Comparison
   Compare the list of assets with penetration testing and VA reports to the list of tactics and techniques used by threat source groups.
4. Conducting Risk Assessment
   Calculate the probability, impact, risk value, and risk level for each identified tactic and technique.
5. Recommendations
   After conducting the risk assessment, provide recommendations based on the assessment.

Proposed Threat Model & Cyber Risk Management

Based on the literature review of various frameworks utilized in previous research studies, this study aims to combine the recommendations of NIST SP 800-30 Rev 1 regarding the Guide for Conducting Risk Assessments with the MITRE ATT&CK Based Analytics Development Method. The following provides an overview of the integration of Risk Assessment into the risk assessment phase using the analytic development method based on the MITRE ATT&CK model. Combine as shown in Figure 2.

Fig.2: Proposed Threat & Risk Modeling Framework

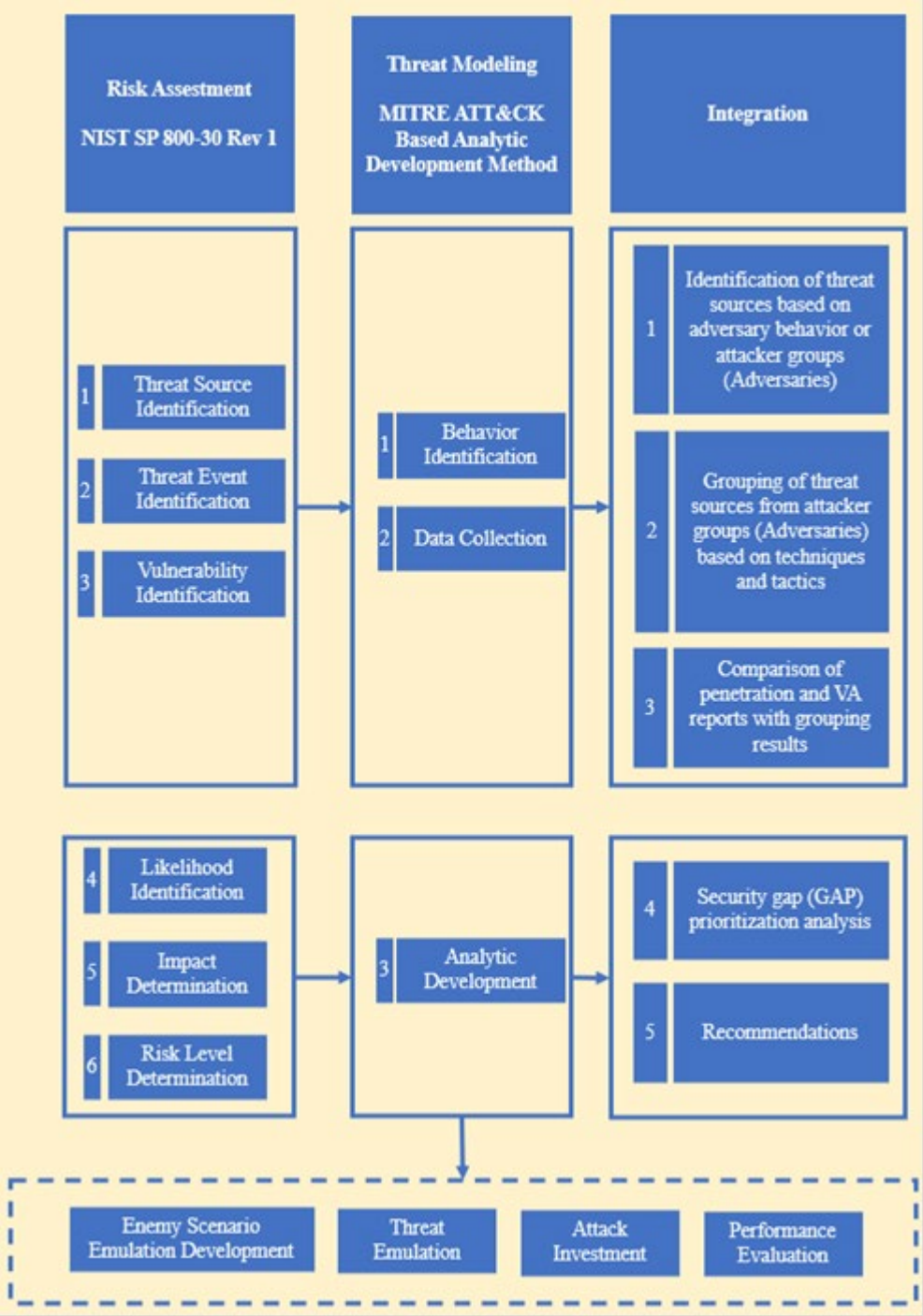

Fig.3: Integration Framework

The integration of Risk Assessment NIST SP 800-30 Rev 1 and Threat Modeling with the MITRE ATT&CK Based Analytic Development Method represents a holistic approach to managing information security risks and analyzing potential threats. It combines two distinct frameworks to understand, identify, and address information security risks effectively. Here's an explanation of how this integration works:

Risk Assessment NIST SP 800-30 Rev 1: This framework provides a structured approach to cybersecurity risk assessment. It encompasses various steps, including threat analysis, vulnerability assessment, probability analysis, impact determination, and control analysis. It helps organizations identify and manage risks systematically.

MITRE ATT&CK Based Analytic Development Method: MITRE ATT&CK is a global knowledge source that catalogs tactics, techniques, and procedures used by attackers in cyberattacks. The analytic development method based on MITRE ATT&CK allows organizations to understand how attackers operate and provides insights into the tactics they might employ in an attack.

The integration process involves the following steps:

- Identification of Threat Sources Based on Attacker Groups: This step involves identifying specific attacker groups that may target an organization. These groups are identified based on real-world observations and historical data.
- Grouping Threat Sources by Attacker Groups Based on Tactics and Techniques: Once the attacker groups are identified, this step classifies them based on the specific tactics and techniques they use. This categorization helps in understanding the modus operandi of these groups.
- Comparison: This step compares the list of assets within the organization with the results obtained from penetration testing and vulnerability assessment (VA) reports. It seeks to match the identified tactics and techniques used by threat source groups with potential vulnerabilities within the organization.
- Conducting Risk Assessment: After matching tactics and techniques with vulnerabilities, a comprehensive risk assessment is conducted. This assessment calculates the probability and impact of potential attacks, resulting in risk values and risk levels for each identified tactic and technique.
- Recommendations: Based on the risk assessment results, recommendations are formulated. These recommendations provide guidance on how to develop effective mitigation strategies and prioritize security measures.

The integration of these two frameworks enables organizations to create a more comprehensive and structured approach to understanding, identifying, and managing information security risks. It empowers organizations to proactively address potential threats, protect critical assets, and enhance their overall cybersecurity posture.

3.1. Initial Condition Identification

In this stage, identification is carried out to gain an overview of the service processes within the organization. Observations are conducted within the government organization to understand the business processes of the services provided. The observation aims to capture the list of services, IT assets, and the identification of existing threats within the organization's service processes.

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

In this stage, the identification of potential threat sources or adversaries to an organization, in this case, a government entity, is conducted. This approach utilizes existing knowledge within the MITRE ATT&CK framework. The steps for identifying threat sources based on the identification of adversary behavior or groups are as follows:

a. Identification of the Targeted Industry:

This process involves specific searches for adversary groups that focus on the government sector.

b. Mapping in MITRE ATT&CK:

Visit https://attack.mitre.org/ and search with the keyword "Government." Identify relevant adversary groups from the search results.

c. Narrowing Down to the Target Industry Region:

In this step, further filtering is done by restricting the adversary groups actively conducting attacks in the Asian region.

These steps help in identifying adversary groups that are specifically targeting the government sector, providing a focused perspective on potential threats.

3.3. Grouping of Threat Sources by Adversary Groups Based on Tactics and Techniques

After the list of adversary groups has been identified, the next step is the grouping of threat sources based on adversary tactics and techniques. Here are the steps involved:

a. Mapping in MITRE ATT&CK using ATT&CK Navigator:

- Access ATT&CK Navigator at https://mitre-attack.github.io/attack-navigator/
- Choose layers and then select the desired matrix; this will display the layer tabs.
- In the selection control, choose "search & multiselect," then select threat groups based on the list of adversary groups.
- Adjust the technique control, assigning a score of 1 for each threat group mapped in the navigator.
- Repeat the steps for selecting layers based on the number of threat groups.
- After each threat group has its own layers, select "new tab" in the layer selection step, then choose "create layer from other layer." Fill in the score expression for each previously created layer according to the threat group.
- Customize the layer controls as needed.
- These layers can be downloaded in JSON and Excel formats for further heatmap generation based on tactics and techniques commonly used by the threat groups.

b. Determining CVSS Scores:

After obtaining information about tactics and techniques, the next step is to determine CVSS (Common Vulnerability Scoring System) scores. This is done using a CVSS calculator by inputting the appropriate metrics based on vulnerabilities. The score ranges from 0 to 10, with higher scores indicating more severe vulnerabilities. Understand the metrics that contribute to the Base Score, including Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, and Availability.

3.4. Comparison of penetration and VA reports with grouping results

In this stage, the information obtained from penetration testing and vulnerability assessment reports will be aligned with the tactics and techniques identified as potential threats by adversary groups. The goal is to identify the correlation between the tactics and techniques used by adversary groups in their attacks with the vulnerabilities detected in the organization's infrastructure or systems. Here are the steps that can be taken in this stage:

- Identify Vulnerabilities:

Compile a list of vulnerabilities detected from penetration testing and vulnerability assessment reports. These vulnerabilities are at the system level, including those within the services of the organization.

- Identification with Tactics and Techniques:

From the list of vulnerabilities in step 1, identify them using the MITRE ATT&CK framework to obtain the IDs of tactics and technique. These IDs can then be compared with the list of tactics and techniques used by adversary groups.

After obtaining the list of vulnerabilities and identifying them to obtain IDs of tactics and techniques using the MITRE ATT&CK framework, the next step is to match them with the list of tactics and techniques used by adversary groups, as conducted in the stage of grouping threat sources based on adversary tactics and techniques. This involves comparing the identified vulnerabilities with the tactics and techniques generated from the grouping of adversary groups.

3.5. Security gap (GAP) prioritization analysis

Next is a crucial stage in conducting threat & risk modeling, which aims to assess the vulnerabilities identified in the government organization. The main objective is to identify, assess risks, and prioritize

security gaps that need to be addressed promptly to reduce potential risks. In the risk assessment process, based on research by (Al Fikri et al., 2019), if there is a match, risk assessment related to vulnerabilities that can be exploited by tactics and techniques from adversary groups will be conducted. This involves assessing the likelihood of an attack occurring and its potential impact. For the criteria of the likelihood of an attack as shown in Table.1, the potential impact as shown in Table 2, and the risk level assessment as shown in Table 3.

Table 1. List of Likelihood Identification Values

Likelihood Identification		
Likelihood Level	Value	Likelihood Identification Criteria
High	3	x >= 3 times in 1 year
Medium	2	1 x >= 2 times in 1 year
Low	1	x <= 1 times in 1 year

Table 2. List of Impact Identification Values

Impact Identification	
Impact Level	Value
High	CVSS Score x Likelihood Value = (51 - 100)
Medium	CVSS Score x Likelihood Value = (11-50)
Low	CVSS Score x Likelihood Value = (1-10)

Table 3. List of Risk Level Assessment

Risk Level Matrix		Likelihood Value		
		High (3)	Medium (2)	Low (1)
Impact Value	High (51-100)			
	Medium (11-50)			
	Low (1-10)			

3.6. Recommendations

The final stage of this research is to provide recommendations based on the previous analysis. These recommendations will include actions to address the identified security gaps and steps that can be taken to enhance cybersecurity risk management within the organization.

4. Result

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

The phase of identifying potential threat sources from attacker groups (Adversaries) is conducted by leveraging the general knowledge available within the MITRE ATT&CK framework at https://attack.mitre.org/ . A search is performed using the keyword "Government" to identify relevant attacker groups in the "groups" section. There are 41 lists of attacker groups that target attacks on the government sector. Subsequently, further filtering is carried out from this list to narrow down attacker groups that are actively conducting attacks in the Asia region. with the results as the identification of threat sources in Table 4:

Table 4. List of mapping government industry attack groups in the Asia region

No	ID Groups	Groups Name	Information
1	G0138	Andariel	Targeting government and companies in South Korea.
2	G0016	APT29	Targeting government networks and research institutions in North America, Europe, Asia, and the Middle East.
3	G0060	BRONZE BUTLER	Targeting organizations in Japan, particularly the technology sector.
4	G0142	Confucius	Targeting prominent individuals, governments, and businesses in South Asia.
.	G…..	…….	……..
17	G0081	Tropic Trooper	Targeting government, healthcare, transportation, and technology industries in Taiwan, the Philippines, and Hong Kong.

4.2. Grouping of threat sources from attacker groups (Adversaries) based on techniques and tactics

After mapping the threat actor groups targeting government and industry sectors in the Asian region, the next step is to perform matrix mapping using the ATT&CK Navigator tool (https://mitre-attack.github.io/attack-navigator/) to obtain the tactics and techniques used by creating layers for each threat actor group according to the list. There are 13 tactics and 475 techniques applied from the 17 listed threat actor groups. From the results of the matrix mapping of tactics and techniques, 10 most frequently used techniques are selected from the list of threat actor groups, which also have high CVSS scores. Here are the results of the list of tactics and techniques used by the attacker groups in Table 5:

Tabel 5. List of Tactics and Techniques by Attacker Groups

No	ID Tactic	Tactic Name	ID Techniques	Techniques Name	Attacker Groups	CVSS Score	Number of Groups
1	TA0001	Initial Access	T1566	Phishing	Andariel, APT29, BRONZE BUTLER, Confucius, Higaisa, Leviathan, menuPass, Mustang Panda, Naikon, Sidewinder, The White Company, Tonto Team, Tropic Trooper's	8,1	13
2	TA0002	Execution	T1204	User Execution	Andariel, APT29, BRONZE BUTLER, Confucius, Higaisa, Leviathan, menuPass, Mustang Panda, Naikon,Sidewinder, The White Company, Tonto Team, Tropic Trooper's	7,5	13

.	T…..	……	……	……	……	……	……
10	TA0011	Command and Control	T1105	Ingress Tool Transfer	Andariel, APT29, BRONZE BUTLER, Confucius, Leviathan, menuPass, Mustang Panda, Sidewinder, Tonto Team,Tropic Trooper's	8,5	10

4.3. Comparison of penetration and VA reports with grouping results

The comparison of penetration testing and vulnerability assessment reports with the grouping results is carried out through the following steps:

a. Vulnerability Identification:
   During the vulnerability identification step, based on interviews and observations, it is revealed that for organization security testing is conducted at least once a year. This testing includes either penetration testing or vulnerability assessment. The list of vulnerabilities based on penetration testing or vulnerability assessment reports is compiled.
b. Identification with Tactics and Techniques:
   After compiling the list of vulnerabilities from penetration testing or vulnerability assessment reports, the next step involves mapping these vulnerabilities using the general knowledge available in the MITRE ATT&CK framework at https://attack.mitre.org/. A search is performed using the keyword "Vulnerabilities" to identify corresponding tactics and techniques.
c. Comparison of Vulnerability List with Tactics and Techniques against Attacker Group Tactics and Techniques:
   Upon obtaining the list of vulnerabilities with their associated IDs from the MITRE ATT&CK framework, a comparison is conducted between the vulnerabilities and the tactics and techniques listed in the attacker group tactics and techniques. The result is a list of tactics and techniques identified from attacker groups, representing their threat model.

4.4. Security gap (GAP) prioritization analysis

Once the list of GAPs (vulnerabilities) in the threat model is identified, the next step is to conduct risk assessment and prioritize security gaps that need to be addressed swiftly to mitigate potential risks. with the results as the identification of threat sources in Table 6.

Tabel 6. List of Security Gap Prioritization Analysis Results

No	Aset Name	Finding	Vulnerability	Threat Model				CVSS Score	Risk Assesment			
				ID Tactic	Tactic Name	ID Techniques	Techniques Name		Likelihood Identification	Impact	Risk Value	Risk Level
1	A 1	HTTPHEADER	X-Content-Type-Option Header	TA0002	Execution	T1203	Exploitation for Client Execution	9,3	3	27,9	83,7	High
2	A 2	Appendix	APACHE 2.4.37 CVE FINDINGS CVE-2019-0211	TA0002	Execution	T1059	Command and Scripting Interpreter	7,8	1	7,8	7,8	Low
..	A…	..	..	..	..	..	..	..	..	..	..	..
10	A 3	Appendix	APACHE 2.4.6 CVE FINDINGS CVE-2017-7679	TA0002	Execution	T1203	Exploitation for Client Execution	9,3	1	9,3	9,3	Low

4.5. Recommendations

Based on the results of the analysis from the aforementioned tables, here are some recommendations that can be implemented:

a. Prioritize High-Risk Assets:
   Focus mitigation efforts on assets with high risk values, such as "A 1" with an average risk score of 51.4. Identify and address potential vulnerabilities in these assets with appropriate security measures.
b. Strengthen Security for "PORTSCAN" Findings:
   "PORTSCAN" ranks first in average risk score with 58.5. Ensure to monitor and mitigate port scanning activities that could pave the way for further attacks. Implement firewalls and other security measures to reduce potential risks.
c. Address "FINGERPRINTING" and "HTTPHEADER" Findings:
   These findings have high average risk scores of 42.9 and 34.3 respectively. Enhance monitoring and detection to identify system mapping and information gathering attempts that could be exploited by attackers.
d. Emphasize Vulnerability Management:
   "SQL Injection" findings have a high risk score with an average of 34.0. Ensure that applications and systems are thoroughly tested to identify and mitigate potential SQL injection vulnerabilities that could jeopardize data and system integrity.
e. Importance of SSL/TLS Management:
   Although "SSL/TLS" has an average risk score of 25.4, it ranks fifth in the findings list. Ensure the security of encryption layers by following best practices in SSL/TLS management, and ensure the use of valid and up-to-date certificates.
f. Prioritize Mitigation for "HTTPHEADER" and "Appendix":
   These findings have a significant number of occurrences across multiple assets. Consider effective mitigation actions to reduce risks associated with these findings, including implementing appropriate header settings and tighter monitoring of related entities.
g. Implement Control Measures:
   Given the CVSS formula considers control factors, ensure the organization has proper control measures in place, including stricter monitoring, regular patch implementation, and appropriate security reinforcement.
h. Early Monitoring and Detection:
   Implement a robust monitoring system to detect suspicious activities or potential threats on assets and findings with high-risk values. Early detection can help prevent attacks before they compromise the system.
i. Enhance Security Awareness:
   Improve security awareness and training for all users and relevant personnel. This can help reduce risks associated with social engineering attacks and enhance overall organizational security.
j. Mitigation
   The following is a table of mitigations for the tactics and techniques that have been identified as targeting the government sector industry.

Table 7. Table Mitigation

Tactic	**Execution**	Technique	**T1204: User Execution**
Mitigation	**User Education:** Educate users about the risks of downloading and running content from untrusted sources. Encourage skepticism towards email attachments and unexpected links. **Email Filtering:** Implement email filtering solutions capable of detecting and blocking phishing emails containing malicious attachments or links.		

	Endpoint Protection: Install and maintain state-of-the-art endpoint security solutions capable of detecting and blocking known malicious code execution attempts. **Disable Macros:** Configure Microsoft Office applications to disable macros by default, reducing the risk of unintentional macro execution. **Web Filtering:** Use web filtering technology to block access to known malicious websites or prevent suspicious content downloads.		
Tactic	**Initial Access**	Technique	**T1204: User Execution**
Mitigation	**User Education:** Train users to recognize phishing indicators, such as suspicious senders, unexpected attachments, and requests for sensitive information. **Email Filtering**: Implement robust email filtering solutions to detect and block phishing emails before they reach users' inboxes. **Multi-Factor Authentication (MFA):** Require the use of MFA to add an additional layer of security, making it harder for attackers to access compromised accounts. **Web Filtering**: Use web filtering tools to block access to known malicious websites commonly used in phishing attacks. **Patch and Update:** Keep software, operating systems, and security software up to date to address known vulnerabilities that attackers may exploit.		
Tactic	…..	Technique	….
Mitigation	…..		
Tactic	**Execution**	Technique	**T1059: Command and Scripting Interpreter**
Mitigation	**Application Whitelisting:** Apply application whitelisting to control the execution of scripts and interpreters, allowing only approved scripts to run. **Least Privilege:** Restrict user privileges to reduce the potential impact of malicious scripts or commands. **Antivirus and Endpoint Detection:** Use antivirus and endpoint detection solutions to scan for known malicious scripts and suspicious behaviors. **Script Analysis:** Implement behavior-based analysis of scripts to detect suspicious or abnormal activity. **Logging and Monitoring:** Monitor command-line activities and script execution for unusual or unauthorized actions. **Disable Unnecessary Features:** Disable or limit access to unnecessary script interpreters and CLI tools for normal business operations. **Patch and Update:** Keep script languages and interpreters up to date to address known vulnerabilities		

By following these recommendations, organizations can minimize risks associated with identified threats and attacks in the MITRE ATT&CK analysis and build a safer and more resilient cybersecurity environment.

5. Conclusion

Based on the conducted research, several conclusions can be drawn as follows:
This research successfully identified various threats and techniques used by attackers in the government environment. By utilizing MITRE ATT&CK as a framework, various attack techniques were analyzed and grouped based on related assets and findings.

a. Comprehensive Threat and Technique Identification:
This research has successfully identified a wide array of threats and techniques employed by attackers within government environments. Leveraging the MITRE ATT&CK framework, the study meticulously analyzed various attack techniques, categorizing them based on related assets and findings. Through the examination of 17 adversary groups, a total of 13 tactics and 475 techniques were identified, shedding light on the complexity of attack strategies employed by these groups. Notably, this research highlights the prevalence of 10 techniques frequently used by these adversaries, characterized by high CVSS scores, signifying the substantial risks associated with their exploitation. These encompass a spectrum of approaches, ranging from social engineering techniques like Phishing to execution-based methods such as User Execution and Exploitation for Client Execution. Additionally, techniques related to the Command and Control phase, such as Ingress Tool Transfer and Application Layer Protocol,

were revealed. Prioritizing the analysis and defense strategies around these techniques emerges as a pivotal step in enhancing resilience and detection against cyberattacks. In-depth familiarity with the most commonly utilized techniques empowers organizations to refine their defense mechanisms, thus reducing potential harm from these attacks.

b. Comprehensive Risk Assessment:
The research has employed the Common Vulnerability Scoring System (CVSS) and consistent risk analysis methods to evaluate the potential impact and risks associated with each asset and finding. This systematic approach enables organizations to determine appropriate mitigation priorities and implement targeted security measures. By assessing the average risk score for each asset and finding, the research aids organizations in identifying and prioritizing the most effective mitigation strategies. Assets and findings with higher risk scores demand heightened attention and mitigation efforts to mitigate potential vulnerabilities effectively.

c. Security Level Based on Findings:
The research has classified findings based on their average risk score, providing valuable insights into the security level of each analyzed attack technique. This categorization facilitates the evaluation of the significance of each technique in the context of cybersecurity risk management.

d. Mitigation and Security Measures Recommendations:
This analysis conducted in this research serves as a solid foundation for generating recommendations aimed at enhancing mitigation strategies and security measures. These recommendations span from improved vulnerability management to the implementation of robust security controls. They offer actionable insights to organizations seeking to mitigate risks effectively.

e. Directing Security Strategy:
By identifying the most prominent threats and techniques, this research equips organizations with valuable insights to formulate more focused and effective security strategies. This, in turn, enables the strategic allocation of investments and resources to safeguard critical assets and data effectively.

f. Contribution to Threat Modeling Knowledge:
This research significantly contributes to the field of threat modeling by demonstrating the immense value of integrating well-established NIST and MITRE ATT&CK frameworks. This integration enhances the precision and comprehensiveness of risk assessment.

g. Practical Application:
The proposed methodology provides government security practitioners with a structured yet adaptable approach to identify and prioritize critical threats and vulnerabilities specific to their organizations. This approach equips them with valuable tools to bolster their cybersecurity posture.

h. Limitations and Future Research:
It's important to note the limitations of this research, such as the reliance on a single organizational sample, which restricts the generalizability of findings. Future research endeavors could focus on validating the integrated framework through broader applications across government agencies and various industries. Additionally, practical future work may involve the development of software tools to automate and streamline elements of the integrated analysis process, facilitating wider adoption and usability.

Therefore, this research serves as a cornerstone in understanding and addressing cyber threats within government environments. By comprehensively identifying threats, assessing risks, and offering targeted mitigation strategies, it equips organizations with the knowledge and tools necessary to navigate the increasingly complex and pervasive cyber threat landscape effectively. Furthermore, its contributions to threat modeling knowledge and practical applicability make it a valuable resource for government security practitioners and researchers alike.

References

Adam Shostack. (2014). *Threat Modeling: Designing for Security*.

Ahmed, M. G., Panda, S., Xenakis, C., & Panaousis, E. (n.d.). MITRE ATT & CK-driven Cyber Risk Assessment. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23â•fi26, 2022, Vienna, Austria* (Vol. 1, Issue 1). Association for Computing Machinery.

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Keamanan siber indonesia 2022. (2022).

Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gupta Gourisetti, S. N. (2020). Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. *2020 Resilience Week (RWS)*, *75*, 106–112. https://doi.org/10.1109/RWS50334.2020.9241271

Nickels, K. (n.d.). *Getting Started with ATT&CK*.

NIST. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Guide for Conducting Risk Assessments*, *September*, 95.

Ponomareva, O. A., Stepanenko, D. V., & Chernova, O. V. (2023). Modeling Features Threats to the Security of Information in the Process Threat Hunting. *2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 305–308. https://doi.org/10.1109/USBEREIT58508.2023.10158844

Potteiger, B., Martins, G., & Koutsoukos, X. (2016). Software and attack centric integrated threat modeling for quantitative risk assessment. *Proceedings of the Symposium and Bootcamp on the Science of Security*, 99–108. https://doi.org/10.1145/2898375.2898390

Shi, Z., Graffi, K., Starobinski, D., & Matyunin, N. (2022). Threat Modeling Tools: A Taxonomy. *IEEE Security & Privacy*, *20*(4), 29–39. https://doi.org/10.1109/MSEC.2021.3125229

Sion, L., Van Landuyt, D., Wuyts, K., & Joosen, W. (2019). Privacy Risk Assessment for Data Subject-Aware Threat Modeling. *2019 IEEE Security and Privacy Workshops (SPW)*, 64–71. https://doi.org/10.1109/SPW.2019.00023

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969

Ucedavélez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118988374

Verreydt, S., Sion, L., Yskout, K., & Joosen, W. (2022). Relationship-based threat modeling. *Proceedings of the 3rd International Workshop on Engineering and Cybersecurity of Critical Systems*, 41–48. https://doi.org/10.1145/3524489.3527303

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157–177. https://doi.org/10.1007/s10270-021-00898-7

Zahid, S., Mazhar, M. S., Abbas, S. G., Hanif, Z., Hina, S., & Shah, G. A. (2023). Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. *Internet of Things*, *22*, 100766. https://doi.org/10.1016/j.iot.2023.100766