សាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ

ROYAL UNIVERSITY OF PHNOM PENH

ប្រធានបទរបាយការណ៍ស្រាវជ្រាវ

Dynamic Adaptive of Ransomware Defense Profile Using Attack Defensive Framework

A Research Report
In Partial Fulfilment of the Requirement for the Degree of
Bachelor of Science in Information Technology Engineering

PANN VICHHKA

July 2022

សាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ

ROYAL UNIVERSITY OF PHNOM PENH

ប្រធានបទរបាយការណ៍ស្រាវជ្រាវ

Dynamic Adaptive of Ransomware Defense Profile Using Attack Defensive Framework

A Research Report
In Partial Fulfilment of the Requirement for the Degree of
Bachelor of Science in Information Technology Engineering

PANN VICHHKA

Examination committee: Dr. SRUN SOVILA (Head of Department ITE)
Mr. NA SAMBATHCHATOVONG

July 2022

ABSTRACT

Nowadays, the cyber landscape is driven by two seemingly contradictory forces: connectivity and fragmentation. On the one hand, advances in technology have made connectivity more than ever which could make to potential cyber-attack threats. The impact from cyber-attack into organization is very a big lose than ever that make cyber-attacks become the first priority scope of the most industry and organization. A Defense framework offer numerous ways to protect systems and infrastructure from threats, however difference defense frameworks could make cybersecurity practitioners hard to decision which one is better to implement on organization. Attack-defense framework is a new proposal which could resolve this issue by combination two difference frameworks into one framework which could using together. Cybersecurity practitioner could be used in technical perspective implement and standard guideline perspective for big cover implementation.

SUPERVISOR’S RESEARCH SUPERVISION STATEMENT

TO WHOM IT MAY CONCERN

Name of program: Bachelor of Information Technology Engineering
Name of candidate: PANN VICHHKA

Title of research report: Dynamic Adaptive of Ransomware Defense Profile Using Attack Defensive Framework

This is to certify that the research carried out for the above titled bachelor’s research report was completed by the above named candidate under my direct supervision. This thesis material has not been used for any other degree. I played the following part in the preparation of this research report: ....

Supervisor's name: NA SAMBATHCHATOVONG

Supervisor’s signature:………………………..

Date……………………………………………

CANDIDATE’S STATEMENT

TO WHOM IT MAY CONCERN

This is to certify that the research report that I Pann Vichhka
hereby present entitled ”Dynamic Adaptive of Ransomware Defense Profile Using Attack Defensive Framework ”

for the degree of Master of Science at the Royal University of Phnom Penh is entirely my own work and, furthermore, that it has not been used to fulfill the requirements of any other qualification in whole or in part, at this or any other University or equivalent institution.

No reference to, or quotation from, this document may be made without the written approval of the author.

Signed by Pann Vichhka: …………………………

Date: ……………………………………………….

Sign by Supervisor: ………………………………..

Supervisor’s signature: …………………………..…

Date……………………………………………..……

Sign by Supervisor: ……………………………..…..

Supervisor’s signature: …………………………...…

Date………………………………………………..…

ACKNOWLEDGEMENT

In this research cannot finished without support and encouragement from different people. And I would like to respect and appreciation to the following people.

Firstly, I would like to thanks and respect to my supervisor, Na Sambathchatovong, who has supported, comment, feedbacks, encouragement and show the way how the research could be success. His advice was showing me that how could I do the research that could be clearer and on time.

Then I would like to show my respect to all my lecturers that I have worked with and study. They also give me the strong knowledge foundation and also soft skill that was an important part which could help my work was done with the good quality.

Finally, I would like to show my deepest and warmest thanks to my family and friends that allow me to living in the good environment and caring about my health during my final year in the bachelor degree. The recovery is my power that could make the action into my research progress.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Background to the Study

In recently year, ransomware [1] attacks continued to be one of the most prominent threats targeting business and organizations worldwide. High-profile attacks disrupted operations of companies in various sectors. According to the 2021 Malware Report by Coresecurity [2], the top three ways previous ransomware breaches had entered the surveyed organizations were phishing emails [3] (70%), email attachments (54%), and users visiting malicious and compromised websites (41%). While spam filters can prevent some of these phish from making it to the inbox and firewalls can block some of these website, social engineering attacks now appear so genuine and realistic that more than a few will slip through the cracks. Ransomware gangs are not only becoming more technologically sophisticated but are also extensively leveraging the growing cybercrime ecosystem looking to find new partners, services and tools for their operations. Most of day, Organization using only one framework and standard to comply or implement the security control into infrastructure against cyber-attack.

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation’s state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations. MITRE ATT&CK [4] become a widely used in cyber defense but also cyber threats also used for their tactics and techniques based across the entire attack lifecycle. For instance, because MITRE ATT&CK takes the perspective of the adversary, security operations teams can more easily deduce an adversary’s motivation for individual actions and understand how those actions relate to specific classes of defenses. On the other hand, Countless organizations around the world use the NIST cybersecurity framework. It helps them assess current cybersecurity status, set goals, and establish standard processes. Moreover, NIST cybersecurity framework [5] also can be used as a cyber risk assessment tool to finding the potential cyber risk willing happens in the organization while MITRE ATT&CK being used in a part of technical works.

1.2 Problem Statement

MITRE ATT&CK is a free tool that private and public sector organizations of all sizes and industries have widely adopted. Users include security defenders, penetration testers, red teams, and cyberthreat intelligence teams as well as any internal teams interested in building secure systems, application, and services. Unlike other models written from a defender's perspective, MITRE ATT&CK intentionally take how adversaries' approach, prepare for, and successfully execute attacks. On the other hand, NIST Cybersecurity framework helps business of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. Both frameworks are a defences framework, however both frameworks are very different perspective. MITRE ATT&CK are used in technical perspective and NIST Cybersecurity framework are used in standard perspective. Ransomware is a software which is built using many methods and tactics. Mostly ransomware gangs also depend on MITRE ATT&CK to form their pre-attack and cyber kill chain techniques into their ransomware software from initialize access to impaction. To defence from the threat actors by complying standard method, it's hard to puzzle which point to implement or not easy to implement at all points while it spends much budget for implement. A single framework control maybe in sufficient to provide solutions to a category by itself; therefore, combination between MITRE ATT&CK and NIST Cybersecurity framework are essential to addressing this problem because once use in technical level and another once use in compliance level.

1.3 Objectives and study

There is a possible way which both frameworks can provide countermeasures by linking MITE ATT&CK and NIST Cybersecurity framework. So, the aim of this study is to create a ransomware defensive profile by mapping MITRE ATT&CK framework to NIST Cybersecurity framework to provides a set of guidelines from NIST Cybersecurity framework to remediation a potential risk willing happens from ransomware attack. The objectives of the research are described as following:

- Briefly understand of MITRE ATT&CK Matrix and NIST Cybersecurity framework
- Review all related work on NIST Cybersecurity framework
- Build an Attack-defense framework by mapping MITRE ATT&CK Matrix to NIST Cybersecurity framework.
- Build a ransomware defensive dynamic profile by using Attack-defense framework.

1.4 Scope and Limitation

Our scope is focusing on:

- Using WannaCry ransomware as a sample based for experimental with new attack-defense framework diagram
- Mapping from ransomware behaviour tactics to a set of guidelines NIST Cybersecurity framework

1.5 Structure of Study

The following is a breakdown of the report's structure. We begin with introduction to ransomware trend and difference perspective of both MITRE ATT&CK Matrix and NIST Cybersecurity framework In the chapter 1. For In Chapter 2, we present more details about definition and structural of both MITRE ATT&CK and NIST Cybersecurity framework. In Chapter 3, the methodology of how attack-defense framework.

CAHPTER 2

LITURATURE REVIEW

2.1 The Definition of MITRE ATT&CK Framework

The MITRE ATT&CK framework is a sophisticated matrix of tactics and approaches used by threat hunters, red teamers, and defenders to properly categorize assaults and estimate the risk of an organization.

The framework's focus is to enhance post-compromise recognition of adversaries in companies by displaying the steps an attacker may have performed. How did the intruder get in? How are they getting around? The knowledge base is intended to assist answer those queries while also raising awareness of an organization's security posture at the perimeter and beyond. Organizations may use the methodology to identify defensive gaps and prioritize them depending on risk.

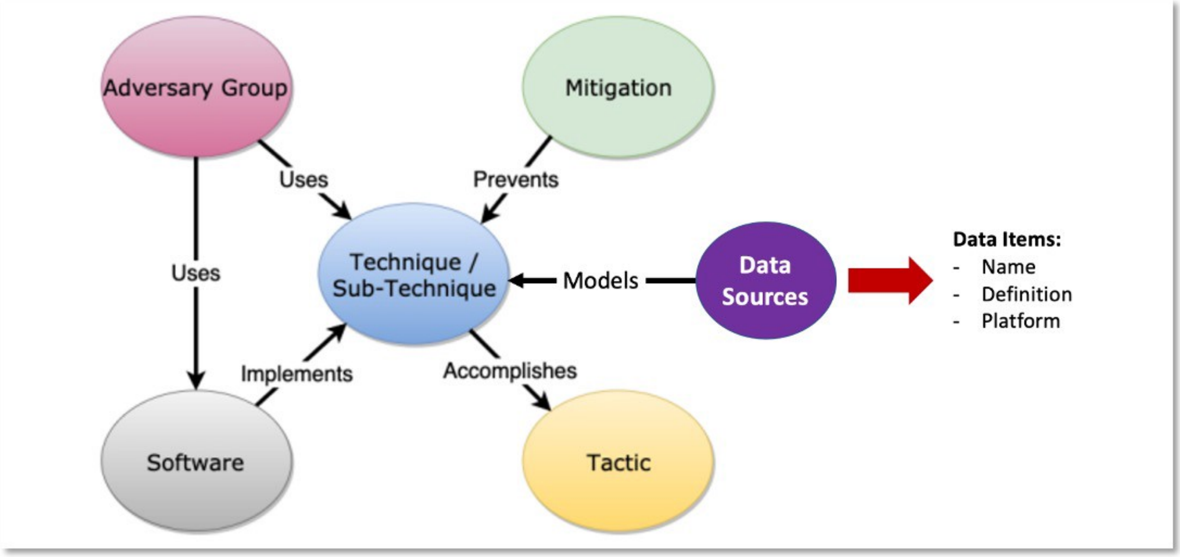


Figure 1: MITRE ATT&CK Object Model with Data Source Object

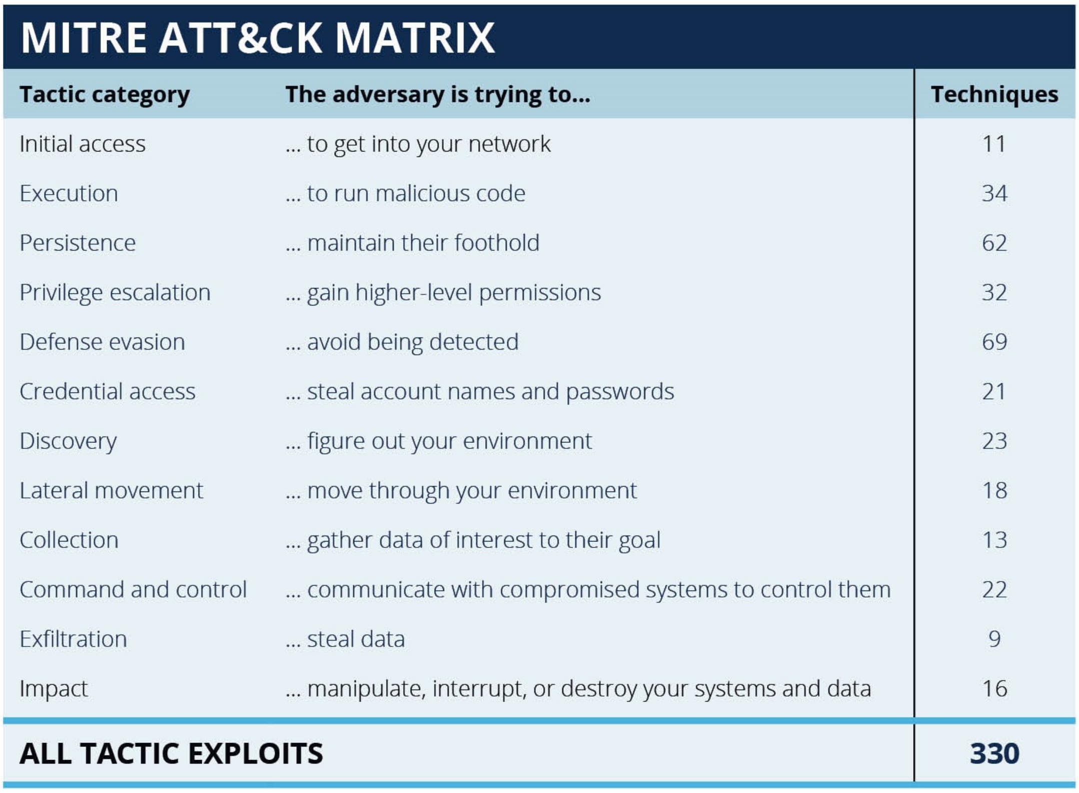
2.1.1 MITRE ATT&CK Tactics, techniques, and mitigation

Adversarial tactics are specific technical objectives that an adversary intends to achieve. For instance, MITRE ATT&CK currently have 14 tactics cataloged in the enterprise matrix:

- Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support the target.
- Resource development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.
- Initial access consists of techniques that use various entry vectors to gain their initial foothold within a network
- Execution consists of techniques that cause attacker-controlled code to be executed locally or remote system.
- Persistence includes techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
- Privilege escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
- Defense evasion includes techniques that adversaries use to avoid detection throughout their compromise.
- Credential access consists of techniques for stealing credentials like account names, and passwords.
- Discovery has techniques an adversary may use to gain knowledge about the system and internal network.
- Lateral movement has a various technique that adversaries use to enter and control remote systems on a network.
- Collection consists of techniques adversaries may use to gather information and the source information is collected from that are relevant to following through on the adversary's objectives.
- Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.
- Exfiltration consists of techniques that adversaries may use to steal data from your network.

- Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

A technique is the way that adversary may try to achieve an objective of attacking or weaponize. A lot of techniques are documented under each tactics category.



MITRE ATT&CK MATRIX

Tactic category	The adversary is trying to…	Techniques
Initial access	… to get into your network	11
Execution	… to run malicious code	34
Persistence	… maintain their foothold	62
Privilege escalation	… gain higher-level permissions	32
Defense evasion	… avoid being detected	69
Credential access	… steal account names and passwords	21
Discovery	… figure out your environment	23
Lateral movement	… move through your environment	18
Collection	… gather data of interest to their goal	13
Command and control	… communicate with compromised systems to control them	22
Exfiltration	… steal data	9
Impact	… manipulate, interrupt, or destroy your systems and data	16
ALL TACTIC EXPLOITS		**330**

Figure 2: MITRE ATT&CK - Tactics

MITRE ATT&CK currently identifies 188 techniques and 379 sub-techniques for enterprise [6]. MITRE ATT&CK covers not only tactics and techniques but also MITRE ATT&CK also provide detection and mitigation for each technique that adversary used.

2.2 The Definition of NIST Cybersecurity Framework

NIST is an acronym that stands for the National Institute of Standards and Technology. Founded in 1901, NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Initially, Congress established NIST to address a major challenge that was obstructing U.S. industrial competitiveness. Following an executive presidential order, NIST published the NIST Compliance Framework in 2014. The order directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and best practices—to reduce cyber risks to critical infrastructures and help organizations build, strengthen, and manage their cybersecurity program. The framework provides a common language so that individuals–from experts to generalists–across the organization have a shared understanding of their cybersecurity risks. It also addresses how an organization can reduce risks and respond to and recover from an attack.

2.2.1 NIST Cybersecurity Core Functions

The NIST Cybersecurity framework uses a simple structure with just give 5 key functions: Identify, Protect, Detect, Respond, and Recover.

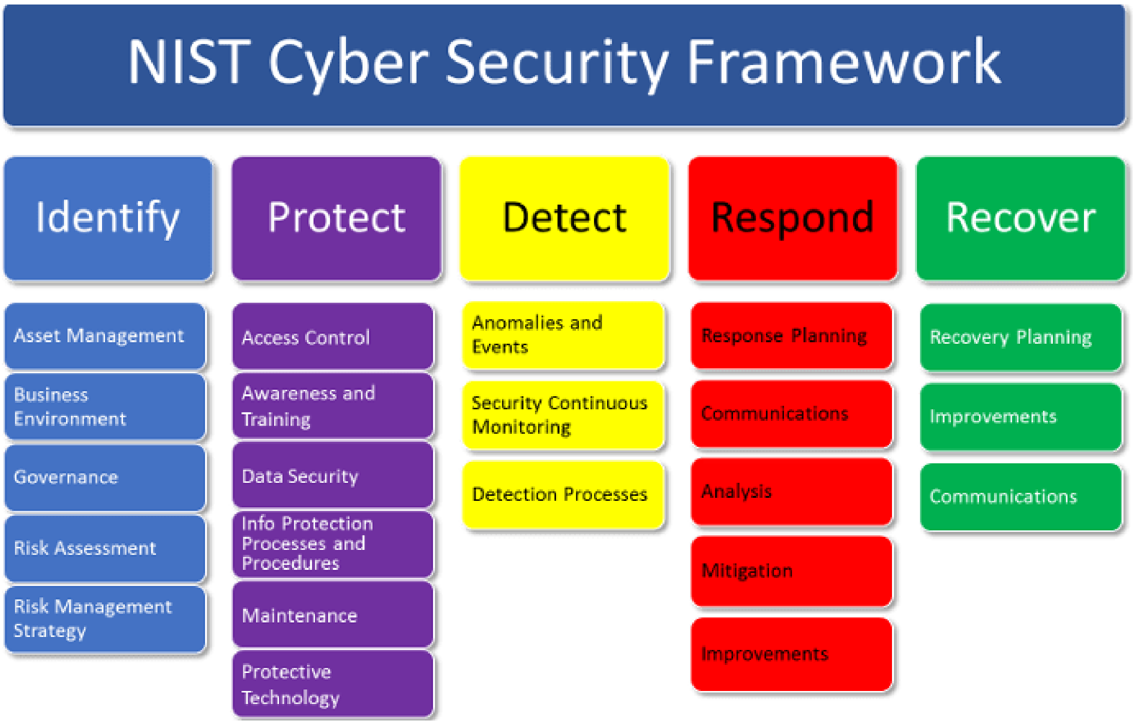
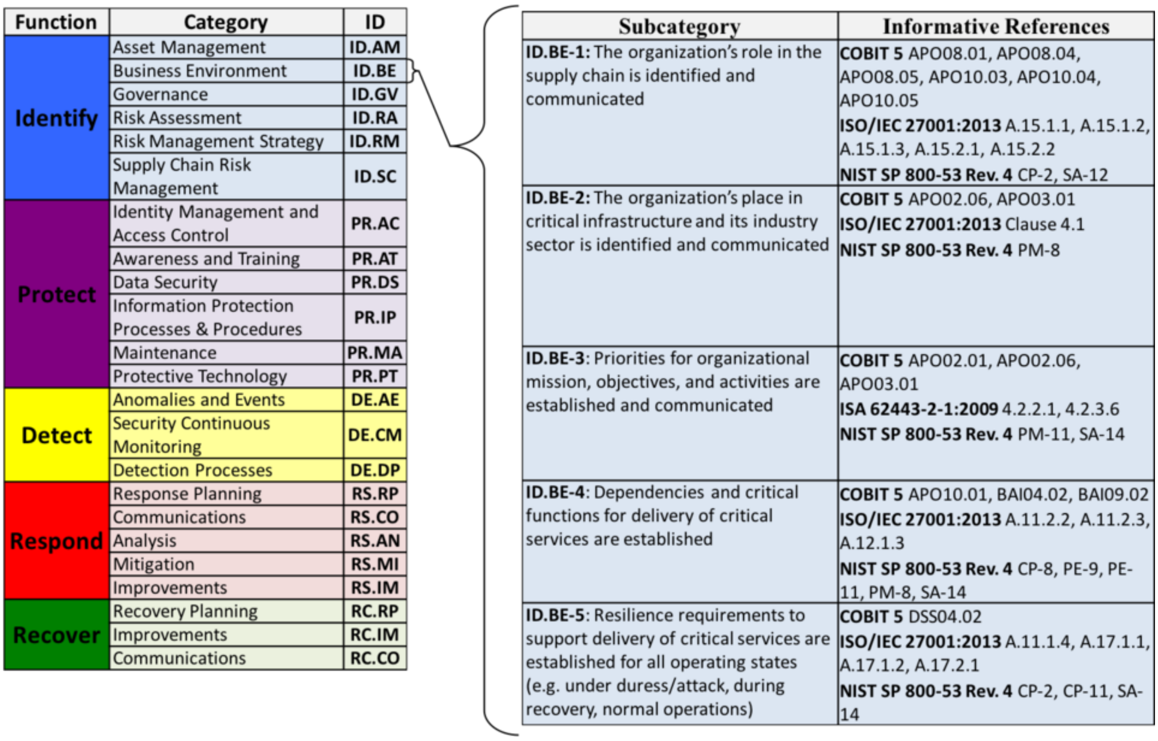


Figure 3: NIST Cybersecurity Framework Structure

Each function uses clear, outcome-based language without extensive technical detail.

- Identify is a function help us to develop an overall risk management approach to cybersecurity. It helps us to understand our critical assets, business environment, governance model, and supply chain.
- Protect is a function help us put important defensive controls in place based on our critical assets, risk tolerance, and other input from the identify function. Protect highlights the importance of managing identities, securing access, protecting data, and training users.

- Detect is when we are under attack, we may not always know right away. The Detect function shortens the time to discovery by spotting anomalies, investigating events, continuously monitoring, and other detection processes.
- Respond is when we know we are under attack, we have to act fast. Response helps us take the right action immediately through incident response planning, analysis, mitigation, communication, and ongoing improvement.
- Recover is when we have stopped the attack, we need to get back to normal. The recover function helps us restore operations through recovery planning, continuous improvement, and communications.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 4: NIST Cybersecurity informative references

NIST Cybersecurity framework provides a wide range of defense mechanisms using 100+ cyber defense controls in 5 above domains. Both of them also updated based on trends of new cyber threats that occur every year.

2.3 Related Works

Since MITRE ATT&CK and NIST Cybersecurity Framework is widely used and adopted, there are some of research papers also propose using each of them in difference ways. [6] M. Mylrea, S. N. G. Gourisetti and A. Nicholls explicate the applicability of buildings cybersecurity framework based on NIST Cybersecurity framework in different types of buildings such as residential, small commerical, large commercial, and federal buildings. [7] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie and S. N. Gupta Gourisetti introduce a tool which offers approaches and practical solutions which enables effective responses against cyber-attacks operational technology (OT) by mapping systematic defensive mechanisms using MITRE ATT&CK Matrix with Facility Cybersecurity Framework (FCF). [8] S. Boudko and H. Abie propose a dynamic cybersecurity framework and investigated adavanced adaptive security to anticipate and respond to dynamic and adaptive attacks on healthcare critial infrastructures. [9] N. Teodoro, L. Gonçalves and C. Serrão presents a basedline for developing a generic and flexible model for manipulating key factors inside organizations: HR, processes and technology, and extraplate the percentage of compliance with the NIST Cybersecurity framework. [10] Mesker, K., Engineer, I. C. develop an ICS Cybersecurity risk assessment using NIST Cybersecurity framework. And [11] Georgiadou, A., Mouzakitis, S. using Cybersecurtiy framework for assessing MITRE ATT&CK. We see that there are many methodologies and flexible to get difference outcome with both of framework.

CHAPTER 3

METHODOLOGY

3.1 How MITRE ATT&CK Works

In Figure 1, the full meaning of MITRE ATT&CK are MITRE Adversarial tactics, Techniques, and Common Knowledge. Adversarial Group can be an attacker, nation state, red teamer which will using the techniques to assesses security or simulate the attack following their cyber kill chain tactics. Another way, Adversarial Group can weaponize their software like ransomware or malware which implement all of stages in their tactics. In defensive perspective, every technique, MITRE Also provides a detection and mitigation for prevention. A security operation teams can be detecting an adversarial group behaviour and analysis their software to evaluation the defensive gap and adversarial group's tactics and techniques. How many steps that adversarial group produces? What techniques is executed? What data source can be impacted? And how to responses and recovery when the system is compromised? These processes are how attractive and defensive is works in MITRE ATT&CK.

3.2 How NIST Cybersecurity Framework Works

In The NIST cybersecurity framework, there are three primary components:

- Core is desired cybersecurity outcomes organized in hierarchy and aligned to more detailed guidance and controls
- Profiles is alignment of an organization's requirements and objectives, risk appetite and resources using the desired outcomes of the framework core
- Implementation Tiers a qualitative measure of organizational cybersecurity risk management practices

In our proposal idea, we will only use The NIST cybersecurity framework core for mapping with MITRE ATT&CK Matrix. As we have introduced NIST Cybersecurity framework core at the CHAPTER 2 already. It establishes a common language with five functions: identify, protect, detect, respond and recover. In depth, following Figure 5 each function has more category and each category has other sub category and, in each subcategory, has an informative reference for providing a guideline or best practice following a standard or compliance. In Functions organize aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk, management decisions, addressing threats, and improving by learning from previous activities. Furthermore, it also aligns with existing methodologies for incident management and help show the impact of investments in cybersecurity. Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Subcategories further divide a Category intro specific outcomes of technical and /or management activities. It provides a set of results which support achievement of the outcomes in each Category. Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

3.3 Mapping MITRE ATT&CK to NIST Cybersecurity Framework

MITRE ATT&CK catalogs about nearly 400 cyber-attack tactics and over 1000 strategies for detection and mitigation the listed of attacks. Mapping all attack and defense tactics to NIST Cybersecurity framework is a polynomial-time to process. And In this section we presents the methodology and process from extact mitigation and detection from MITRE ATT&CK to cybersecurity activities in NIST Cybersecurity framework.

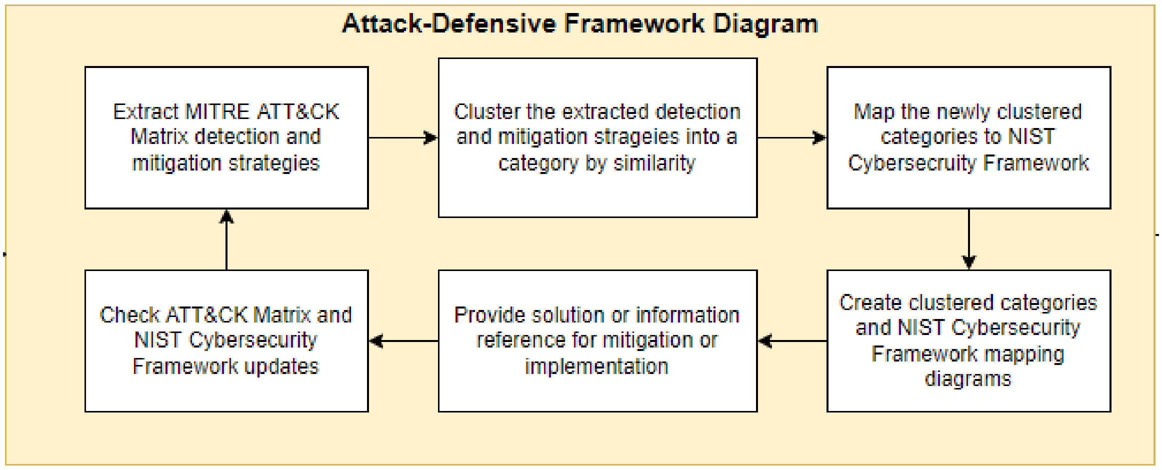

Attack-Defensive Framework Diagram
Extract MITRE ATT&CK Matrix detection and mitigation strategies
Cluster the extracted detection and mitigation stragieies into a category by similarity
Map the newly clustered categories to NIST Cybersecruity Framework
Create clustered categories and NIST Cybersecurity Framework mapping diagrams
Provide solution or information reference for mitigation or implementation
Check ATT&CK Matrix and NIST Cybersecurity Framework updates

Figure 5: Mapping MITRE ATT&CK to NIST Cybersecurity Framework diagram

3.3.1 Extract MITRE ATT&CK Matrix Mitigation and Detection

Firstly, detection and mitigation mechanisms for all cyber-attack tactics and techniques which presented in ATT&CK Matrix were extracted. In general, each technique always provides the possible mitigation and detection in many ways. Table I show the part of how mitigation and detection were extracted. In Create or Modify System Process techniques, there are many mitigations and detection were provided such as audit, behavior prevention on endpoint, code signing etc.

Table 1: The extraction of mitigation and detection from MITRE ATT&CK Matrix

Create or Modify System Process	Mitigation	Audit
		Behavior Prevention on Endpoint
		Code Signing
		Limit Software Installation
		Operating System Configuration
		Restrict File and Dictionary Permissions
		User account management
	Detection	Command
		Driver
		File
		Process
		Service
		Windows Registry
Exploitation of Remote Services	Mitigation	Application Isolation and Sandboxing
		Disable or remove feature or program
		Exploit protection
		Network Segmentation
		Privileged account

		management
		Threat Intelligence program
	Detection	Application Log
		Network Traffic

3.3.2 Clustering Mitigation and detection into a new category

The next step is to recategorize all of the listed mitigation and detection techniques which has similar attributes or behavior into a new category. For example, In Table I Behavior prevention on Endpoint and exploit protection are all re-categorized under new category Prevention & Protection in Table 2. All mitigations and detections techniques were grouped as sub categories of new main categories according to their similarities.   For the new categories is created is based on mitigation and detection similarity could be matched. In case, how to identify is based on user experience or cyber security practitioner understanding all these mitigation and detection works.

Table 2: The extraction of mitigation and detection from MITRE ATT&CK Matrix

Category	**Sub-Category**
Audit	Audit
Prevention & Protection	Behavior Prevention on Endpoint
	Exploit Protection
Validation or checksum	Code signing
Limitation	Limit software installation
	Disable or remove feature or program
Configuration	Operating System Configuration
Privilege & Permission	Restrict File and Dictionary Permissions
Account management	User account management
	Privileged account management
Intelligence capability	Threat Intelligence program

Logging	Command
	Driver
	File
	Process
	Service
	Windows Registry
	Application Log
	Network Traffic

3.3.3 Mapping the Newly Clustered Categories to NIST Cybersecurity Framework

A Controls in NIST Cybersecurity framework provide a set of activities or guidelines checklist and an approach to problem solving related to cybersecurity incidents. Furthermore, NIST Cybersecurity framework suggests information references such as CIS Control, ISO, COBIT, and NIST to apply the control by these practical defense mechanisms. A single activates may be insufficient to provide control solutions to a new clustered category, therefore, multiple activities control combinations can essentially address that problem. For example, a combination activities DE.AE-3 (Event data are collected and correlated from multiple sources and sensors) and DE.CM-7 (Monitoring for unauthorized personnel, connections, devices, and software is performed) produces a more effective guideline for mitigation command & control through monitoring all system activities also include network traffic. In Table 3 show an example of mapping a new clustered categories to NIST Cybersecurity framework activities.

Table 3: Mapping new clustered categories to NIST Cybersecurity framework

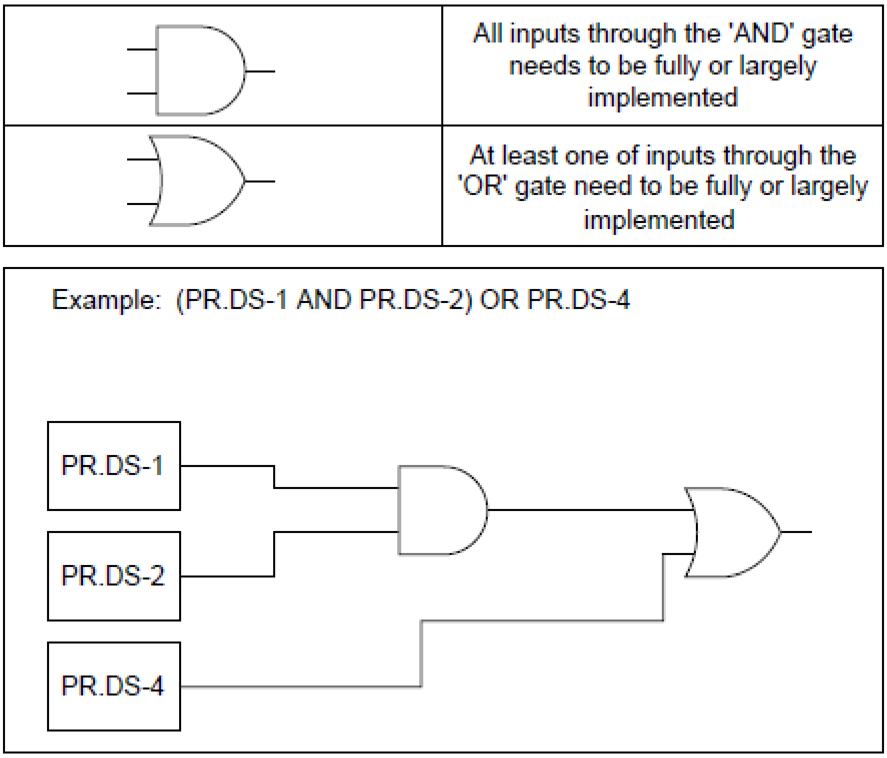
Category	Sub-Category	NIST Cybersecurity Framework
Audit	Audit	**PR.DS-6**: Integrity checking mechanisms are used to verify software, firmware, and information integrity AND **PR.DS-8**: Integrity checking mechanisms are

		used to verify hardware integrity AND **PR.PT-1**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy AND **DE.CM-8**: Vulnerability scans are performed AND **PR.AC-1**: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Prevention & Protection	Behavior Prevention on Endpoint	**ID.SC-1**: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders AND (**PR.DS-1**: Data-at-rest is protected AND **PR.DS-2**: Data-in-transit is protected) OR **PR.DS-4**: Adequate capacity to ensure availability is maintained AND **PR.PT-2:** Removable media is protected and its use restricted according to policy AND **DE.AE-2**: Detected events are analyzed to understand attack targets and methods AND (**DE.CM-4**: Malicious code is detected OR **DE.CM-5**: Unauthorized mobile code is detected) AND **DE.CM-7**: Monitoring for
	Exploit Protection	

		unauthorized personnel, connections, devices, and software is performed
Validation or checksum	Code signing	**PR.DS-6**: Integrity checking mechanisms are used to verify software, firmware, and information integrity
Limitation	Limit software installation	**PR.PT-3**: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
	Disable or remove feature or program	
Configuration	Operating System Configuration	**PR.PT-3**: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities AND **PR.IP-3**: Configuration change control processes are in place
Privilege & permission	Restrict File and dictionary permissions	**PR.AC-4**: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
Account management	User account management	**PR.AC-4**: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties AND **PR.IP-3**: Configuration change control processes are in place
	Privileged account management	
Intelligence capability	Threat Intelligence program	**ID.RA-2**: Cyber threat intelligence is received from information sharing forums and sources
Logging	Command	**ID.AM-3**: Organizational communication and data flows are mapped AND **DE.CM-7**: Monitoring for unauthorized personnel, connections, devices, and
	Driver	
	File	
	Process	
	Service	
	Windows Registry	
	Application Log	

	Network Traffic	software is performed

In additional, to listing activities of NIST Cybersecurity framework related to category and sub category as the Table III above, map with AND/OR logic gates are used to present step-by-step activities to mitigation from cyber-attacks. In Figure 6, show the useable of logic gate in a part of prevention & protection, if (DE.CM-4: Malicious code is detected OR DE.CM-5: Unauthorized mobile code is detected) AND DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed, then the potential cybersecurity events will be more likely to be reduced and security control is implemented. More control or implement in a series make adversary harder to get past or break the targeted network and system.



All inputs through the 'AND' gate needs to be fully or largely implemented

At least one of inputs through the 'OR' gate need to be fully or largely implemented

Example: (PR.DS-1 AND PR.DS-2) OR PR.DS-4

Figure 6: Mapping with AND/OR logic gate

In case, to clear the responsibility cyber practitioner must be pickup the recommendation activities and check detail in NIST Cybersecurity framework information reference which provided detail guideline from a various standards and compliances.

CHAPTER 4

RESULT AND DISCUSSION

In this discussion we will using attack-defense framework to test on WannaCry Ransomware. What activities will cybersecurity practitioner do to reduce the potential impact from ransomware.

To begin, firstly we need to collect all malware analysis report about WannaCry to extract all its behaviours to mapping with MITE ATT&CK to identify what tactics and techniques which this software used.

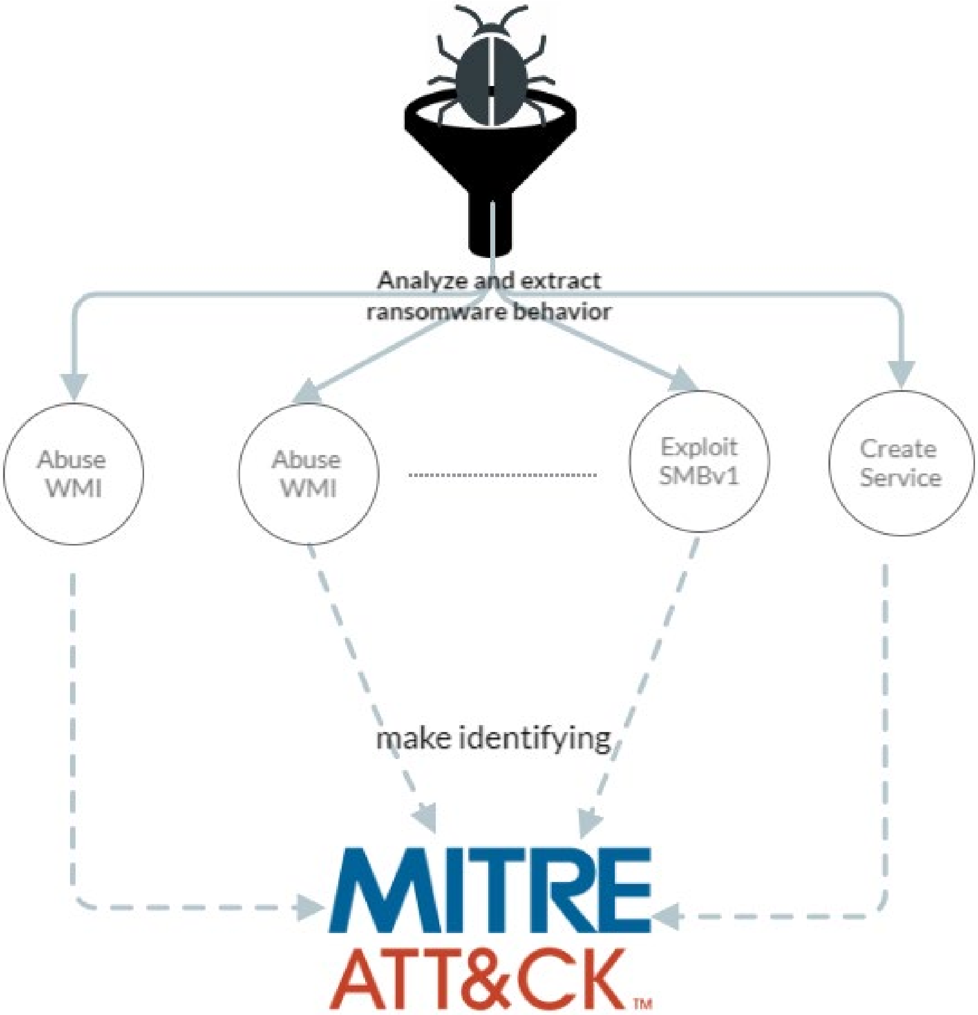
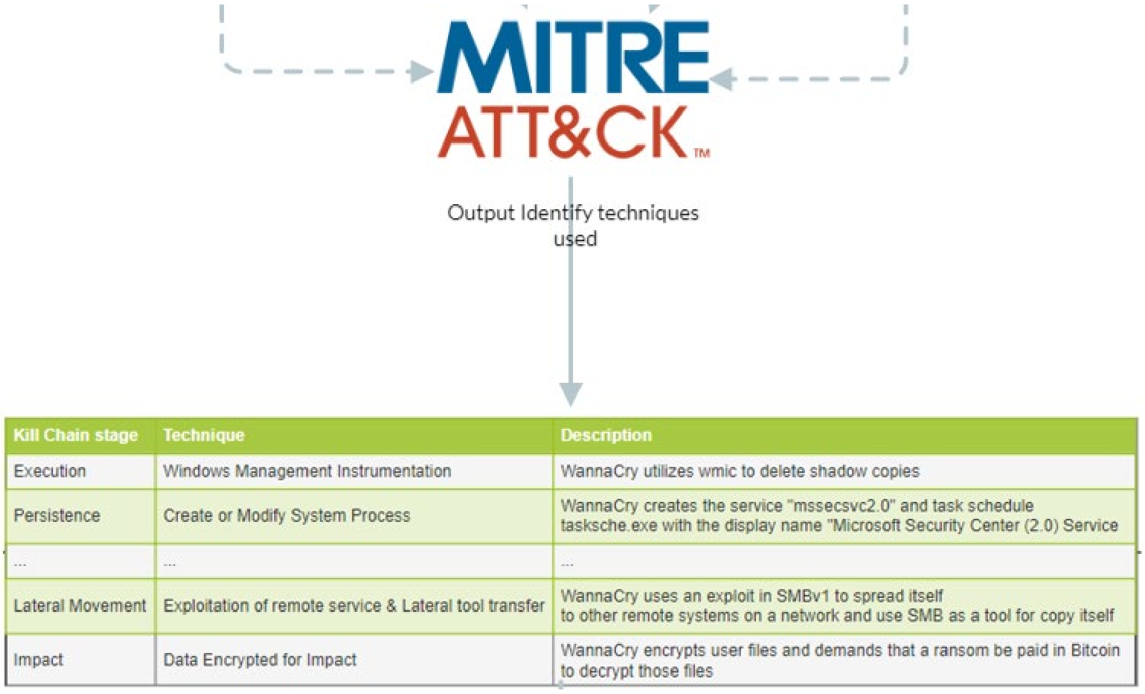


Figure 7: Extract malware behaviours

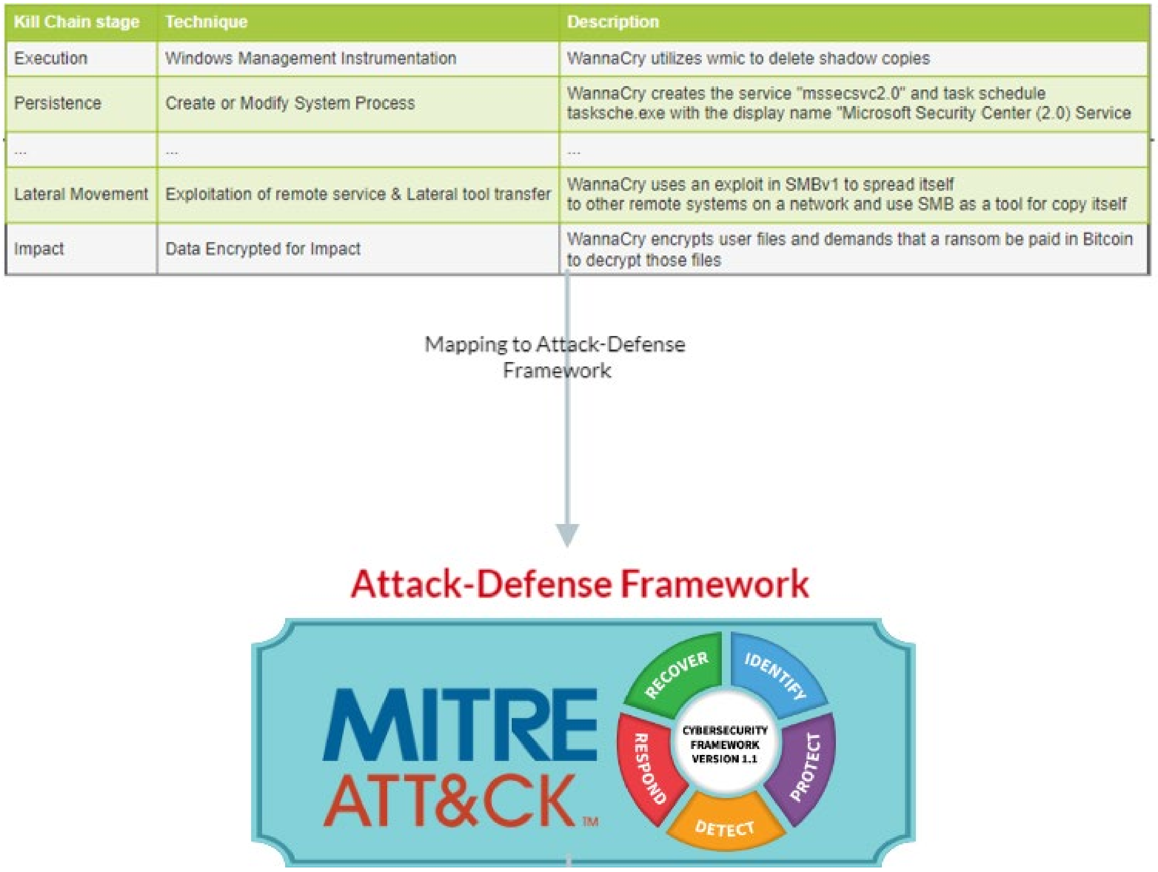
In Figure 7, Cybersecurity practitioner need to collects all malware behaviours from the analyse report. We have shown some sample behaviours of WannaCry such as abuse WMI, Exploitation on SMBv1, create a service to make a persistence running. Then we need to match these behaviours with MITE ATT&CK.



Kill Chain stage	Technique	Description
Execution	Windows Management Instrumentation	WannaCry utilizes wmic to delete shadow copies
Persistence	Create or Modify System Process	WannaCry creates the service "mssecsvc2.0" and task schedule tasksche.exe with the display name "Microsoft Security Center (2.0) Service
...	...	...
Lateral Movement	Exploitation of remote service & Lateral tool transfer	WannaCry uses an exploit in SMBv1 to spread itself to other remote systems on a network and use SMB as a tool for copy itself
Impact	Data Encrypted for Impact	WannaCry encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files

Figure 8: Mapping new clustered categories to NIST Cybersecurity framework

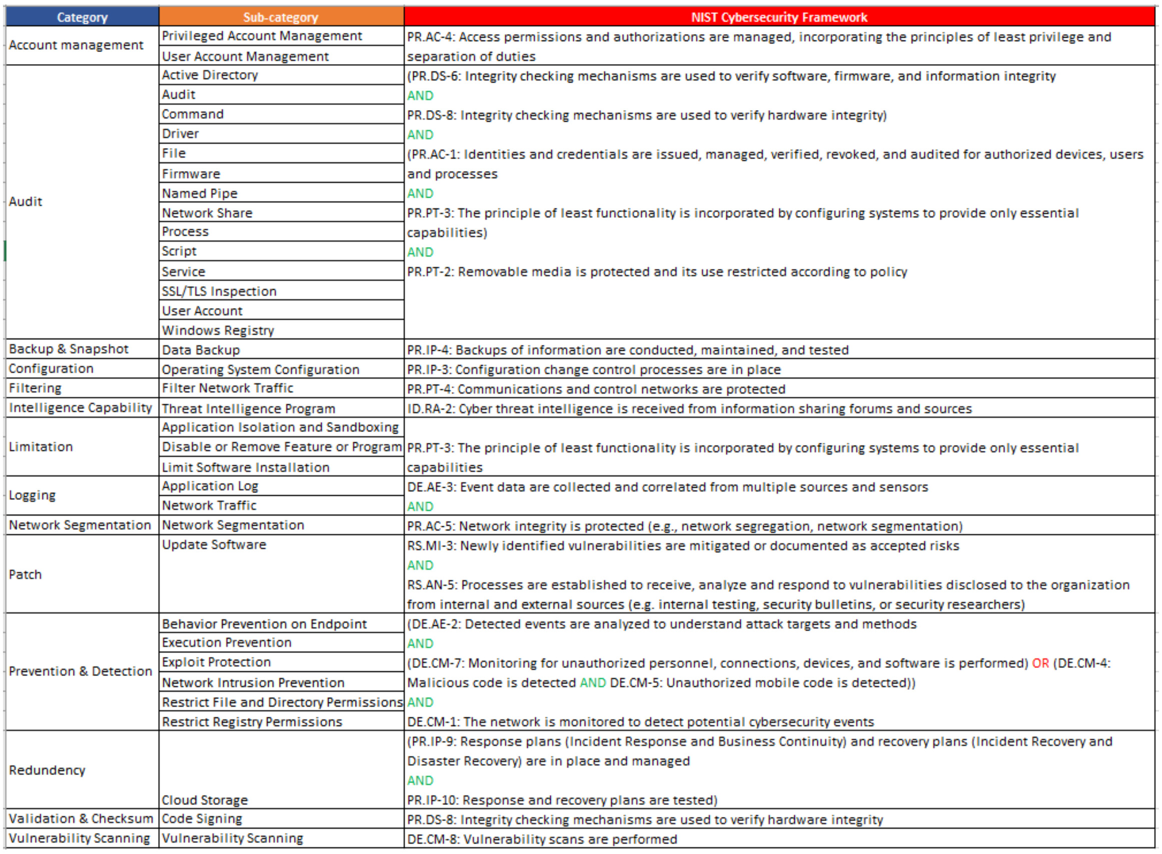
In Figure 8, we show some sample what tactics that attacker was used in their software and each technique what they did when the software start executed. For example, when malware is executed, the malware using Windows management instrumentation techniques to delete shadow file copies which user couldn't recovery that backup files. And much more stage until Impact stage which malware encrypted all files and documents.



Kill Chain stage	Technique	Description
Execution	Windows Management Instrumentation	WannaCry utilizes wmic to delete shadow copies
Persistence	Create or Modify System Process	WannaCry creates the service "mssecsvc2.0" and task schedule tasksche.exe with the display name "Microsoft Security Center (2.0) Service
...	...	...
Lateral Movement	Exploitation of remote service & Lateral tool transfer	WannaCry uses an exploit in SMBv1 to spread itself to other remote systems on a network and use SMB as a tool for copy itself
Impact	Data Encrypted for Impact	WannaCry encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files

Figure 9: Mapping techniques to Attack-Defense Framework

In Figure 9, we collected all techniques that ransomware used to mapping detection and mitigation into Attack-defense framework. In a result we will get a defensive profile as below.



Category	Sub-category	NIST Cybersecurity Framework
Account management	Privileged Account Management	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
	User Account Management	
Audit	Active Directory	(PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity AND PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity) AND (PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes AND PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities) AND PR.PT-2: Removable media is protected and its use restricted according to policy
	Audit	
	Command	
	Driver	
	File	
	Firmware	
	Named Pipe	
	Network Share	
	Process	
	Script	
	Service	
	SSL/TLS Inspection	
	User Account	
	Windows Registry	
Backup & Snapshot	Data Backup	PR.IP-4: Backups of information are conducted, maintained, and tested
Configuration	Operating System Configuration	PR.IP-3: Configuration change control processes are in place
Filtering	Filter Network Traffic	PR.PT-4: Communications and control networks are protected
Intelligence Capability	Threat Intelligence Program	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
Limitation	Application Isolation and Sandboxing	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
	Disable or Remove Feature or Program	
	Limit Software Installation	
Logging	Application Log	DE.AE-3: Event data are collected and correlated from multiple sources and sensors AND
	Network Traffic	
Network Segmentation	Network Segmentation	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
Patch	Update Software	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks AND RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
Prevention & Detection	Behavior Prevention on Endpoint	(DE.AE-2: Detected events are analyzed to understand attack targets and methods AND (DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed) OR (DE.CM-4: Malicious code is detected AND DE.CM-5: Unauthorized mobile code is detected)) AND DE.CM-1: The network is monitored to detect potential cybersecurity events
	Execution Prevention	
	Exploit Protection	
	Network Intrusion Prevention	
	Restrict File and Directory Permissions	
	Restrict Registry Permissions	
Redundency	Cloud Storage	(PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed AND PR.IP-10: Response and recovery plans are tested)
Validation & Checksum	Code Signing	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
Vulnerability Scanning	Vulnerability Scanning	DE.CM-8: Vulnerability scans are performed

Figure 10: Result ransomware defensive profile

CHAPTER 5

CONCLUSION AND FUTUREWORK

In this paper, we study the countermeasure of two framework which could possible combination and provide a set of serries guideline or activates. We convert from doing mitigation and detection technical things to a standard implementation which include the physical activates and system activates to minimize to potential threat that easily could penetrate or exploit the infrastructure. Most of the previous research, both frameworks are very dynamic use in difference environment. Using both frameworks together the cybersecurity practitioner could improve their security control in the infrastructure more effective and specific scope and activities. In case, using the security controls in wrong way, it could be losing the optimization on expending and implementation.

For future, to be use the attack-defense framework in financial industry at Cambodia, we will further work on combination NBC-TRMG (National Bank Cambodia Technology Risk Management Guidelines) into attack-defense framework.

REFERENCES

[1] CISA gov Ransomware 101 available: https://www.cisa.gov/stopransomware/ransomware-101

[2] Coresecurity by HelpSystems 2021, Why Do ransomware Attacks Keep Happening? Available: https://www.coresecurity.com/blog/why-do-ransomware-attacks-keep-happening

[3] Coresecurity by HelpSystems What is Phishing avaiable: https://www.coresecurity.com/penetration-testing/phishing

[4] Crowdstrike May 27,2021, MITRE ATT&CK FRAMEWORK available: https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/

[5] National Institute of Standards and Technology (NIST) April 16, 2018 Framework for Improving Critical Infrastructure Cybersecurity available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[6] M. Mylrea, S. N. G. Gourisetti and A. Nicholls, "An introduction to buildings cybersecurity framework," 2017 IEEE Symposium Series on Computational Intelligence (SSCI), 2017, pp. 1-7, doi: 10.1109/SSCI.2017.8285228

[7] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," 2020 Resilience Week (RWS), 2020, pp. 106-112, doi: 10.1109/RWS50334.2020.9241271

[8] S. Boudko and H. Abie, "Adaptive Cybersecurity Framework for Healthcare Internet of Things," 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), 2019, pp. 1-6, doi: 10.1109/ISMICT.2019.8743905

[9] N. Teodoro, L. Gonçalves and C. Serrão, "NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements," 2015 IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 418-425, doi: 10.1109/Trustcom.2015.402

[10] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. Sensors, 21(9), 3267

[11] Mesker, K., Engineer, I. C., & Chevron, E. T. C. (2014, October). Adapting NIST Cybersecurity Framework for Risk Assessment. In NIST Conference

[12] Delotte, Leading the way with an adversary focus available: https://www2.deloitte.com/us/en/insights/industry/public-sector/government-deter-cybersecurity-adversary.html