CHAPTER I
INTRODUCTION

1.1. Background

In the rapidly evolving digital era, cybersecurity has become a fundamental challenge for the operational continuity of modern organizations [1]. The growing reliance on information systems and computer networks not only provides convenience for users but also presents the risk of increasingly complex and sophisticated cyber threats [2]. Among these various cyber threats, ransomware has emerged as one of the most destructive attacks due to its ability to encrypt critical data, paralyze services, and force victims to pay a ransom amount determined by the attackers [3]. The impact is not only financial but also results in operational disruptions, loss of public trust, and potential regulatory violations [1].

These ransomware incidents continue to rise globally. For example, in the healthcare sector alone, ransomware attacks experienced a surge from 34% in 2021 to 60% in 2023, with an average recovery cost reaching $2.2 million per incident [1]. The increasing scale of these attacks indicates that ransomware has evolved into an increasingly aggressive and difficult-to-control threat. A similar phenomenon is also evident in Indonesia. The National Cyber and Crypto Agency (BSSN) reported over 15 million malware anomalies, including ransomware, in December 2022 alone. Furthermore, ransomware such as LockBit has successfully penetrated various critical sectors in Indonesia, such as the banking sector, raising concerns regarding the readiness of national cyber defenses [3].

The selection of LockBit 3.0 as the primary threat focus in this research is driven by its massive track record of attacks. A joint report from global cyber intelligence agencies released by the Cybersecurity and Infrastructure Security Agency (CISA) explains that LockBit was the most deployed ransomware variant worldwide in 2022 and continued to dominate through 2023. The scale of its attacks dominates globally, with LockBit being responsible for 22% of total ransomware incidents in Canada, 23% in New Zealand, and 18% in Australia during the same period. The high intensity and sophistication of these attacks make LockBit 3.0 a highly relevant modern threat representation to serve as a benchmark in testing the effectiveness of a cyber defense framework [4].

Previous research studying the operational mechanisms of LockBit

ransomware attacks was conducted by [3]. They noted that LockBit is capable of evading detection and disabling built-in system defense mechanisms such as Windows Defender. These increasingly sophisticated attack techniques demand an analytical mechanism capable of explaining how each stage of the attack unfolds systematically. To explain how attacks like LockBit operate, MITRE ATT&CK provides a knowledge base containing the tactics, techniques, and procedures (TTPs) utilized by attackers [2].

As a simpler illustration, the TTP concept can be likened to a planned strategy in a house burglary. Tactics represent the burglar's objective, such as gaining entry into the house. Techniques are the methods selected to achieve that goal, such as sneaking through a window or breaking down a door. Meanwhile, Procedures are the detailed steps along with the specific tools used, for instance, prying the window hinges using a screwdriver at midnight. In a cybersecurity context, utilizing this TTP framework allows for the mapping of the entire sequence of attack activities, enabling organizations to understand attack patterns structurally from start to finish, rather than merely observing the resulting damage.

A structured understanding of these attack patterns is crucial as it serves as the foundation for organizations to determine the appropriate defensive measures. After understanding how attacks are executed through TTPs mapped in MITRE ATT&CK, organizations require a defense framework capable of mitigating risks at every attack stage. One widely adopted framework is CIS Controls, which provides a prioritized list of security controls as a foundation for cyber defense implementation [5]. However, its generic approach results in CIS providing less specific guidance against particular attack techniques, especially when dealing with modern threats that rely on evasion techniques and the utilization of built-in operating system features (*living off the land*) [6].

The limitations of this generic approach prompted the emergence of MITRE D3FEND, a catalog of defense techniques focusing on the direct mapping between attack techniques and defensive mechanisms that can inhibit, detect, or neutralize specific TTPs [7]. With its more precise approach, D3FEND provides a clearer picture of what defensive actions are relevant to counter modern ransomware like LockBit, which employs a series of layered techniques. Unlike frameworks utilizing a general approach, D3FEND emphasizes the causal relationship between attacker activities and

the direct defensive actions that can address them.

Nevertheless, both approaches have their respective limitations. The implementation of CIS Controls in the field is often suboptimal because many organizations fail to implement all controls comprehensively due to resource constraints [8]. Additionally, the empirical validation of this approach remains weak. Recent studies on security control standards reveal a gap where identified attack techniques lack direct mitigation in standard frameworks [9]. Meanwhile, MITRE D3FEND only maps the technical relationship between attacks and defenses, but it does not provide quantitative data regarding how effective these overall techniques are in halting real-world ransomware attacks [10].

This condition highlights a research gap: the absence of studies directly comparing the effectiveness level of a generic approach like CIS Controls against a specific approach like D3FEND in countering modern ransomware attacks. Therefore, this research is proposed to fill this gap. By designing and executing LockBit 3.0 TTP simulation scenarios in a laboratory environment, this study will conduct a quantitative comparison of the effectiveness of a defense configuration enhanced based on CIS Controls and a defense configuration enhanced based on MITRE D3FEND. The results of this research are expected to provide empirical evidence regarding which approach is more effective in mitigating LockBit 3.0 TTPs, as well as offer insights for organizations in selecting the appropriate cyber defense strategy.

1.2. Problem Formulation

Based on the background described above, the following are the research problems to be examined in this comparative study on the effectiveness of cybersecurity frameworks:

1. How to counter the attack stages of LockBit 3.0 ransomware?
2. How effective are defense frameworks in preventing and limiting the attack stages of LockBit 3.0 ransomware?
3. How to determine the most optimal defense approach against the threat of LockBit 3.0 ransomware attack stages?

1.3. Research Objectives

The objectives of conducting this research are as follows:

1. To implement the MITRE D3FEND and CIS Controls frameworks as defense configurations.
2. To analyze the effectiveness of the MITRE D3FEND and CIS Controls frameworks in preventing and limiting the attack stages of LockBit 3.0 ransomware.
3. To compare the effectiveness level of the MITRE D3FEND and CIS Controls frameworks in countering the LockBit 3.0 ransomware threat during its attack stages.

1.4. Research Benefits

The expected benefits from conducting this research are as follows:

1. To enrich the literature related to the evaluation of cyber defense framework effectiveness against LockBit 3.0 ransomware TTPs.
2. To provide an implementation guide for defenses based on D3FEND and CIS Controls that can be directly applied to enhance protection against modern ransomware such as LockBit 3.0.
3. To serve as a reference for organizations in determining security frameworks for ransomware attack mitigation.
4. To broaden the insights and experience of the researcher in implementing and evaluating cybersecurity frameworks, specifically MITRE D3FEND and CIS Controls, in the context of ransomware attacks.

1.5. Research Limitations

To ensure this research is more directed, focused, and does not deviate from the established objectives, the scope of this research is limited to the following:

1. The attack scenarios only cover LockBit 3.0 TTPs (Tactics, Techniques, and Procedures) that can be executed legally.
2. Testing is conducted in a closed virtual laboratory environment, not on production systems or real infrastructure.
3. Testing is conducted using an *Assumed Breach* approach, where the simulation is assumed to begin after the attacker has successfully gained initial access to one of the target machines.