CHAPTER V
CONCLUSION

5.1. Conclusion

Based on the results of the LockBit 3.0 ransomware attack simulation and the comparative analysis conducted using a quantitative approach of 50 iterations for each exploitation tactic, several conclusions can be drawn.

1. In facing the attack stages of LockBit 3.0 ransomware, the MITRE D3FEND and CIS Controls frameworks have been successfully implemented as defensive configuration strategies on the target system. Testing proves that structured LockBit 3.0 attacks require organizations to implement specific defensive settings at the operating system level, ranging from security auditing and network filtering to locking anti-malware features.
2. Based on the effectiveness analysis using the Adversary Technique Coverage (ATC) metric, the MITRE D3FEND framework recorded a mitigation rate of 75%. MITRE D3FEND successfully restricted attacks in the Lateral Movement, Defense Evasion, and Impact phases, but failed to prevent the initial phase of Credential Access due to its passive detection-only approach. Conversely, the CIS Controls framework is proven capable of perfectly and consistently preventing and restricting all attack stages with an effectiveness rate of 100%.
3. After comparing the effectiveness rates of both, the most optimal defensive approach against the threat of LockBit 3.0 ransomware attack stages is the CIS Controls framework. With an effectiveness margin advantage of 25% over MITRE D3FEND, the proactive prevention approach of CIS Controls is proven to be superior because it successfully disrupts the attack chain from the initial stage through the restriction of administrative access privileges.

5.2. Suggestions

Based on the findings and limitations of this study, several suggestions can be considered for future research development and practical implementation in the field.

1. This study focuses solely on the Tactics, Techniques, and Procedures (TTPs) of LockBit 3.0 ransomware. Future research is recommended to test the effectiveness of these two frameworks against other modern Ransomware-as-

a-Service (RaaS) variants, such as BlackCat (ALPHV), Cl0p, or Akira, which possess different propagation characteristics and defense evasion techniques.

2. The testing in this study was conducted only on a standard computer scale running Windows 11. To ensure the results more closely resemble actual conditions in the field, future research is advised to test these defenses on a larger network, for example, using Active Directory on Windows Server. The objective is to observe how effective these frameworks are when deployed directly within real-world corporate network systems.
3. Future research can explore the use of Machine Learning models to automate the mapping of mitigation techniques within the MITRE D3FEND framework. The involvement of AI can focus on developing anomaly detection engines capable of dynamically triggering defensive controls, such as Process Suspension or File Encryption Analysis in D3FEND, as soon as a LockBit attack pattern is detected. Additionally, the use of AI can assist organizations in continuously auditing the implementation of CIS Controls through automated continuous monitoring, allowing security gaps in Group Policy or system configurations to be proactively identified and remediated before being exploited by threat actors.