**UNDERGRADUATE THESIS**

# COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF MITRE D3FEND AND CIS CONTROLS FRAMEWORKS IN MITIGATING LOCKBIT 3.0 TTP ATTACKS

**SYAHBAGUS RADITHYA HARYO SANTOSO**
NPM 22081010255

**THESIS ADVISORS**
Henni Endah Wahanani, ST. M. Kom.
Achmad Junaidi, S.Kom, M.Kom

**MINISTRY OF HIGHER EDUCATION, SCIENCE, AND TECHNOLOGY**
**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR**
**FACULTY OF COMPUTER SCIENCE**
**INFORMATICS STUDY PROGRAM**
**SURABAYA**
**2026**

**APPROVAL SHEET**

**COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF MITRE D3FEND AND CIS CONTROLS FRAMEWORKS IN MITIGATING LOCKBIT 3.0 TTP ATTACKS**

By :

SYAHBAGUS RADITHYA HARYO SANTOSO
NPM. 22081010255

Has been defended before, and accepted by, the Board of Assessors of the Thesis Examination of the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional Veteran Jawa Timur, on May 20, 2026:

**Approved,**

**Henni Endah Wahanani, ST, M.Kom** (Advisor I)
NIP. 19780922 2021212 005

**Achmad Junaidi, S.Kom., M.Kom** (Advisor II)
NIP. 197811102025211048

**Budi Nugroho, S.Kom, M.Kom** (Head Assessor)
NIP. 19800907202121 1005

**Ardhon Rakhmadi, S.Tr.T., M.Kom** (Assessor I)
NIP. 199108052024061002

**Acknowledge by,**

**Dean of the Faculty of Computer Science**

**Prof. Dr. Ir. Novirina Hendrasarie, MT**
**NIP. 19681126 199403 2 001**

**APPROVAL SHEET**

# COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF MITRE D3FEND AND CIS CONTROLS FRAMEWORKS IN MITIGATING LOCKBIT 3.0 TTP ATTACKS

By :

SYAHBAGUS RADITHYA HARYO SANTOSO

NPM. 22081010255

Approved to proceed to the Thesis Examination

**Approved by,**

**Coordinator of Informatics Study Program**

**Faculty of Computer Science**

**Dr. Intan Yuniar Purbasari, S.Kom. MSc.**

**NIP. 198006022025212029**

## STATEMENT OF ORIGINALITY

I am the undersigned:

| | | |
|---|---|---|
| Student Name | : | Syahbagus Radithya Haryo Santoso |
| NPM | : | 22081010255 |
| Degree Program | : | Bachelor (S1) |
| Study Program | : | Informatics |
| Faculty | : | Faculty of Computer Science |

Hereby declare that this undergraduate thesis contains no part of any other scientific work that has been submitted to obtain an academic degree at any higher education institution. Furthermore, it does not contain any work or opinions previously written or published by others, except for those which are explicitly cited in this thesis and listed completely in references.

And I declare that this scientific document is free from elements of plagiarism. If in the future indications of plagiarism are found in this Thesis, I am willing to accept sanctions in accordance with the applicable laws and regulations.

Thus, I made this statement without any coercion from anyone and to be used as it should.

Surabaya, May 20, 2026
Declarant,


SYAHBAGUS RADITHYA H. S.
NPM. 22081010255

## ABSTRACT


| | | |
|---|---|---|
| Student Name / NPM | : | Syahbagus Radithya Haryo Santoso / 22081010255 |
| Thesis Title | : | Comparison of the Effectiveness of MITRE D3FEND and CIS Controls Frameworks in the Mitigation of LockBit 3.0 TTP Attacks |
| Advisors | : | 1. Henni Endah Wahanani, ST, M.Kom<br>2. Achmad Junaidi, S.Kom., M.Kom |



Ransomware remains one of the most critical threats to organizational data integrity, with LockBit 3.0 emerging as a highly sophisticated variant utilizing complex Tactics, Techniques, and Procedures (TTPs). This study evaluates and compares the defensive effectiveness of two prominent cybersecurity frameworks, MITRE D3FEND and CIS Controls, in mitigating LockBit 3.0 attacks. Using a quantitative experimental methodology, the research was conducted within a controlled virtual environment consisting of a Windows 11 target and a Kali Linux attacker. The attack scenario encompassed four critical stages: Credential Access (T1003.002), Lateral Movement (T1021.002), Defense Evasion (T1562.001), and Data Encryption Impact (T1486). The experimental results demonstrated that the baseline system without security implementations was entirely vulnerable (0% effectiveness). Implementing the MITRE D3FEND framework achieved an effectiveness score of 75%, successfully mitigating Lateral Movement, Defense Evasion, and Impact, but failing to prevent Credential Access due to its reliance on passive detection (D3-FA). In contrast, the CIS Controls framework achieved a perfect effectiveness score of 100% by successfully neutralizing the attack at the initial stage through strict access control (CIS Control 5.4). This study concludes that while MITRE D3FEND provides granular defensive mapping, CIS Controls offers a more robust and proactive defense-in-depth strategy against ransomware-based TTPs.



**Keywords**: *LockBit 3.0, Ransomware, MITRE D3FEND, CIS Controls, TTPs, Cybersecurity.*

## ACKNOWLEDGEMENTS

Praise be to Allah SWT for all His graces, guidance, and gifts to the author so that the undergraduate thesis with the title **"Comparative Analysis of the Effectiveness of MITRE D3FEND and CIS Controls Frameworks in Mitigating LockBit 3.0 TTP Attacks"** can be completed properly.

During the preparation of this thesis, the author received a lot of assistance, guidance, and support from various parties. For this, the author would like to thank:

1. Prof. Dr. Ir. Novirina Hendrasarie, M.T. as the Dean of the Faculty of Computer Science, Universitas Pembangunan Nasional "Veteran" Jawa Timur.
2. Dr. Intan Yuniar Purbasari, S.Kom. MSc. as the Coordinator of the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional "Veteran" Jawa Timur.
3. Mrs. Henni Endah Wahanani, ST. M. Kom. as Advisor I, who has provided invaluable guidance, patient advice, and continuous motivation throughout the completion of this thesis.
4. Mr. Achmad Junaidi, S.Kom, M.Kom as Advisor II, who has dedicated his time and expertise to provide critical insights and directions to the author.
5. All Lecturers of the Informatics Study Program, Faculty of Computer Science, for their guidance and knowledge provided during the author's education.
6. My dearest Mother, who has always played an important role in the author's journey, providing continuous material and moral support. She has always been a constant source of comfort and emotional support for the author, and her prayers have been a constant source of strength.
7. My dearest Father, who taught the writer to be responsible, work hard, and never give up easily. His advice and examples are an important foundation for the author in undergoing each process with determination.

The author realizes that in the preparation of this thesis there are many shortcomings. For this reason, constructive criticism and suggestions from all parties are highly expected for the perfection of this writing. Finally, with all the

limitations that the author has, hopefully this report can be useful for all parties in general and the author in particular.

Surabaya, May 20th 2026

Author

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES