



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 :

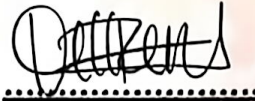
SYAHBAGUS RADITHYA HARYO SANTOSO
NPM. 22081010255

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

NIP. 19780922 2021212 005



(Advisor I)

Achmad Junaidi, S.Kom., M.Kom

NIP. 197811102025211048



(Advisor II)

Budi Nugroho, S.Kom, M.Kom

NIP. 198009072021211005



(Head Assessor)

Ardhon Rakhmadi, S.Tr.T., M.Kom

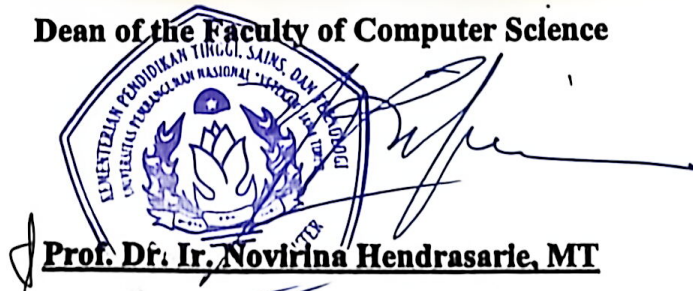
NIP. 199108052024061002



(Assessor I)

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
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

APPROVAL SHEET	iii
APPROVAL SHEET	v
STATEMENT OF ORIGINALITY	vii
ABSTRACT	ix
ACKNOWLEDGEMENTS.....	xi
TABLE OF CONTENTS.....	xiii
LIST OF FIGURES	xvii
LIST OF TABLES	xix
CHAPTER I INTRODUCTION.....	1
1.1. Background	1
1.2. Problem Formulation.....	3
1.3. Research Objectives	3
1.4. Research Benefits	4
1.5. Research Limitations.....	4
CHAPTER II LITERATURE REVIEW	5
2.1. Previous Research	5
2.2. Cybersecurity	8
2.3. Cybersecurity Risk Mitigation	9
2.4. Malware.....	9
2.5. Ransomware	10
2.6. Lockbit 3.0	12
2.6.1. Credential Access (T1003.002 - Security Account Manager)	12
2.6.2. Lateral Movement (T1021.002 - SMB/Admin Shares)	13
2.6.3. Defense Evasion (T1562.001 - Impair Defenses)	14

2.6.4. Impact (T1486 - Data Encrypted for Impact).....	15
2.7. Cybersecurity Framework	15
2.8. TTP.....	16
2.9. MITRE ATT&CK.....	17
2.10. MITRE D3FEND	18
2.10.1. File Analysis (D3-FA).....	20
2.10.2. Network Traffic Filtering (D3-NTF)	21
2.10.3. Application Configuration Hardening (D3-ACH)	21
2.10.4. Local File Access Mediation (D3-LFAM).....	22
2.11. CIS Control	23
2.11.1. CIS Control 05: Account Management.....	24
2.11.2. CIS Control 04: Secure Configuration of Enterprise Assets and Software	25
2.11.3. CIS Control 10: Malware Defenses	26
2.11.4. CIS Control 11: Data Recovery	26
2.12. Effectiveness of Cybersecurity Frameworks.....	27
2.13. Effectiveness Metrics	27
2.14. Tools Used.....	28
2.14.1. VirtualBox.....	28
2.14.2. Windows 11.....	29
2.14.3. Kali Linux	30
2.14.4. Mimikatz	31
2.14.5. Impacket-PsExec.....	31
CHAPTER III METHODOLOGY.....	33
3.1. Research Methodology.....	33
3.2. Research Procedure	33

3.3. Research Tools and Materials	35
3.3.1. Software	35
3.3.2. Hardware	36
3.4. Test Environment Design.....	36
3.4.1. Network Topology	37
3.4.2. Virtual Machine Configuration	38
3.5. Attack Scenario Design Using MITRE ATT&CK	39
3.5.2. Credential Access Scenario: OS Credential Dumping (T1003.002)...	40
3.5.3. Lateral Movement Scenario: SMB/Windows Admin Shares (T1021.002).....	42
3.5.4. Defense Evasion Scenario: Impair Defenses (T1562.001)	44
3.5.5. Impact Scenario: Data Encrypted for Impact (T1486).....	45
3.6. Defense Scenario Using MITRE D3FEND	46
3.6.1. File Analysis Defense Scenario (D3-FA).....	47
3.6.2. Network Traffic Filtering Defense Scenario (D3-NTF)	48
3.6.3. Application Configuration Hardening Defense Scenario (D3-ACH) .	50
3.6.4. Local File Access Mediation Defense Scenario (D3-LFAM).....	51
3.7. Defense Scenario Using CIS Controls	52
3.7.1. CIS Control 05: Account Management Defense Scenario.....	53
3.7.2. CIS Control 04: Secure Configuration Defense Scenario	54
3.7.3. CIS Control 10: Malware Defense Scenario	55
3.7.4. CIS Control 11: Data Recovery Defense Scenario	56
3.8. Experimental Protocol.....	57
3.9. Analysis Method	58
3.9.1. Results Analysis	58
CHAPTER IV RESULTS AND DISCUSSION	61

4.1. Test Environment Implementation.....	61
4.2. Baseline Testing Results	61
4.2.1. Credential Access Attack Results (T1003.002)	62
4.2.2. Lateral Movement Attack Results (T1021.002).....	62
4.2.3. Defense Evasion Attack Results (T1562.001)	63
4.2.4. Impact Attack Results (T1486)	64
4.3. MITRE D3FEND Framework Testing.....	66
4.3.1. File Analysis Defense (D3-FA).....	66
4.3.2. Network Traffic Filtering Defense (D3-NTF)	68
4.3.3. Application Configuration Hardening Defense (D3-ACH)	69
4.3.4. Local File Access Mediation (D3-LFAM).....	71
4.4. CIS Controls Framework Testing	73
4.4.1. Restrict Administrator Privileges Defense (CIS 5.4)	74
4.4.2. Disable Unnecessary Services Defense (CIS 4.8).....	75
4.4.3. Deploy and Maintain Anti-Malware Software Defense (CIS 10.1)....	77
4.4.4. Data Recovery Defense (CIS 11.2)	79
4.5. Analysis of Test Results.....	83
4.5.1. ATC Calculation for MITRE D3FEND	83
4.5.2. ATC Calculation for CIS Controls.....	84
4.5.3. Recapitulation and Comparison	85
CHAPTER V CONCLUSION	87
5.1. Conclusion.....	87
5.2. Suggestions.....	87
REFERENCES.....	89

LIST OF FIGURES

Figure 2.1 MITRE ATT&CK Logo	17
Figure 2.2 MITRE D3FEND Logo	19
Figure 2.3 Oracle VirtualBox Logo	29
Figure 2.4 Windows 11 Logo.....	29
Figure 2.5 Kali Linux Logo.....	30
Figure 2.6 Logo Impacket	32
Figure 3.1 Research Procedure.....	34
Figure 3.2 Network Topology Diagram.....	38
Figure 3.3 Credential Access Scenario	41
Figure 3.4 Lateral Movement Scenario.....	43
Figure 3.5 Defense Evasion Scenario	44
Figure 3.6 Impact Scenario	46
Figure 3.7 File Analysis (D3-FA) Scenario	48
Figure 3.8 Network Traffic Filtering (D3-NTF) Scenario	49
Figure 3.9 Application Configuration Hardening (D3-ACH) Scenario.....	50
Figure 3.10 Local File Access Mediation (D3-LFAM) Scenario	52
Figure 3.11 Account Management Scenario	54
Figure 3.12 Secure Configuration Scenario	55
Figure 3.13 Malware Defense Scenario	56
Figure 3.14 Data Recovery Scenario.....	57
Figure 4.1 Virtual Machines in VirtualBox	61
Figure 4.2 Credential Access Attack Results	62
Figure 4.3 Lateral Movement Attack Results	63
Figure 4.4 Defense Evasion Attack Results (T1562.001).....	64

Figure 4.5 Files Before Encryption.....	65
Figure 4.6 Impact Attack Results (T1486).....	65
Figure 4.7 Successful Mimikatz Execution Accessing SAM	66
Figure 4.8 Attack Detection on Event Viewer (Event ID 4663).....	67
Figure 4.9 Lateral Movement Results Experiencing Connection Timeout.....	68
Figure 4.10 SMB Connection Blocking Logs in Windows Defender.....	69
Figure 4.11 Windows Defender Deactivation Attack Results	70
Figure 4.12 Windows Security Protection Status Post-Attack.....	71
Figure 4.13 Access Denial on the Attacker's Terminal.....	72
Figure 4.14 File Modification Blocking Logs in Protection History	73
Figure 4.15 Downgrading Access Privileges to Standard User (Karyawan)	74
Figure 4.16 Mimikatz Execution Denial Due to Access Privilege Restrictions ...	75
Figure 4.17 Disabling SMB Service on the Victim System.....	76
Figure 4.18 Impacket Execution Failure on the Attacker Terminal.....	77
Figure 4.19 Tamper Protection Configuration on the Victim Machine	78
Figure 4.20 Execution of the Real-time Protection Deactivation Script.....	79
Figure 4.21 Data Backup Implementation to an Isolated Directory	80
Figure 4.22 Primary Directory Successfully Encrypted by the Attacker.....	81
Figure 4.23 Data Recovery Process	82
Figure 4.24 LockBit 3.0 Mitigation Success Comparison Chart	86

LIST OF TABLES

Table 2.1 List of Previous Research.....	6
Table 3.1 List of Tested LockBit 3.0 TTPs.....	40
Table 3.2 Success Indicators for the Credential Access Attack Scenario	42
Table 3.3 Success Indicators for the Lateral Movement Attack Scenario	43
Table 3.4 Success Indicators for Defense Evasion	45
Table 3.5 Success Indicators for Impact	46
Table 3.6 MITRE D3FEND Mapping	47
Table 3.7 CIS Controls Mapping	53
Table 3.8 Comparison of Defensive Framework Effectiveness.....	60
Table 4.1 Defensive Framework Effectiveness Comparison Results	85