

**A CONTEXT-SEMANTIC REAL-TIME PROCESS MONITORING AND
DETECTION FRAMEWORK FOR FILELESS AND LIVING-OFF-THE-LAND
(LOTL) ATTACK**

By

Alan Sufarlan

22451043

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

Revision after the Thesis Defense on February 4, 2026

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Alan Sufarlan

14 February 2026
Date

Student

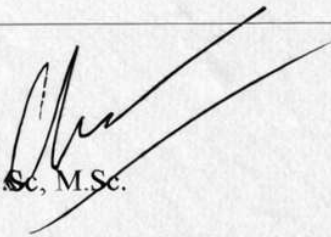
Approved by:



Dr. Ir. Eka Budiarto, ST., M.Sc.

14 February 2026
Date

Thesis Advisor



Dr. Ir. Charles Lim, B.Sc., M.Sc.

14 February 2026
Date

Thesis Co-Advisor

Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc.

Date
Dean

ABSTRACT

A CONTEXT-SEMANTIC REAL-TIME PROCESS MONITORING AND DETECTION FRAMEWORK FOR FILELESS AND LIVING-OFF-THE-LAND (LOTL) ATTACK

By

Alan Sufarlan

Dr. Ir. Eka Budiarto, ST, M.Sc, Advisor

Dr. Ir. Charles Lim, Bsc, M.Sc, Co-Advisor

SWISS GERMAN UNIVERSITY



The increasing prevalence of fileless and Living-off-the-Land (LOTL) attacks poses significant challenges to traditional signature-based security systems due to their stealthy and in-memory execution characteristics. This research proposes a context–semantic real-time detection framework for identifying fileless and LOTL attacks in Windows environments. The framework integrates contextual process behavior features with semantic analysis of command-line and script content, which are fused using a machine learning–based classifier. Experiments conducted in a controlled multi-virtual-machine environment using MITRE ATT&CK aligned datasets demonstrate that the proposed approach achieves high detection performance with low false positive rates while maintaining real-time detection latency. Furthermore, SHAP-based explainability is incorporated to improve transparency and analyst trust. The results indicate that combining contextual and semantic analysis enhances the effectiveness and interpretability of real-time fileless attack detection systems.

Keywords: Fileless Attacks, Living-off-the-Land (LOTL), Explainable AI (XAI)



DEDICATION

This thesis is dedicated to Indonesia, as a contribution to the advancement of cybersecurity knowledge for the nation's future. It is also dedicated to my beloved family for their unconditional support, patience, and encouragement throughout this academic journey. Special appreciation is extended to my friends for their motivation, collaboration, and shared experiences during the completion of this research. Finally, this work is dedicated to my advisors and lecturers, whose guidance, expertise, and invaluable insights made this research possible.



ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all those who have supported and contributed to the completion of this thesis. First and foremost, I am deeply thankful to my family for their unconditional love, patience, and continuous encouragement throughout my academic journey. Their support has been a constant source of motivation.

I would also like to extend my appreciation to my friends for their companionship, constructive discussions, and moral support during this research process. My sincere thanks go to my colleagues for their collaboration, technical insights, and professional support, which greatly enriched this study.

Furthermore, I am profoundly grateful to my thesis advisors and lecturers for their invaluable guidance, expertise, and constructive feedback throughout the research. Their academic supervision played a crucial role in shaping this work.

Finally, I would like to thank the company for providing the resources, environment, and support necessary to conduct this research. This thesis would not have been possible without the collective contributions of all parties involved.

TABLE OF CONTENTS

ABSTRACT	3
DEDICATION	5
TABLE OF CONTENTS	7
LIST OF FIGURES.....	15
LIST OF TABLES	18
CHAPTER 1 - INTRODUCTION	20
1.1. Background	20
1.2. Research Problem.....	21
1.3. Research Questions	24
1.4. Research Objectives	24
1.5. Research Hypotheses.....	25
1.6. Scope and Limitation	25
1.6.1 Scope of the Research	25
1.6.2 Limitations of the Research.....	26
1.7. Thesis Structure.....	26
CHAPTER 2 - LITERATURE REVIEW	28
2.1. Business and Industry landscape.....	28
2.1.1 The Rise of Digital Interdependence.....	28
2.1.2 Threat Actors Targeting Modern Enterprise Systems.....	29
2.1.3 Operational Pressure and Security Complexity	30
2.1.4 Emergence of Stealth-Driven Attacks in Enterprises.....	32

2.1.5 Implication for Malware and Threat Detection Research	33
2.2 Business Challenges: Physical vs Cyber Threats	34
2.2.1 Characteristics of Physical Threats	34
2.2.2 Characteristics of Cyber Threats	35
2.2.3 The Cyber Risk Convergence Problem	36
2.2.4 Why Cyber Threats Now Outweigh Physical Risks	38
2.2.5 Implications for Malware Research	39
2.3 Malware Overview	40
2.3.1 Defining Malware in the Modern Context	40
2.3.2 Evolution of Malware Across Four Eras	41
2.3.3 Malware Classification in Modern Enterprise Environments	43
2.3.4 Malware as a Behavioral Phenomenon	44
2.4 Modern Malware Trends and the Emergence of Fileless Techniques	45
2.4.1 Decline of Traditional File-Based Malware	45
2.4.2 Rise of In-Memory and Script-Based Execution	46
2.4.3 Abuse of Legitimate Administrative Tools (LOLBins)	47
2.4.4 Increased Use of Obfuscation and Encoding Techniques	49
2.4.5 Increased Focus on Stealth and Operational Blending	50
2.4.6 Ineffectiveness of Traditional Detection Models	51
2.4.7 Modern Attack Case Studies Illustrating Fileless Trends	53
2.4.8 Implications for Detection Research	54
2.5 Fileless and Living-off-the-Land (LOTL) Attacks	55
2.5.1 Definition and Characteristics of Fileless Malware	56
2.5.2 Living-off-the-Land (LOTL) Attack Techniques	58
2.5.3 Fileless/LOTL Attack Lifecycle (Detailed Technical Analysis)	59
2.5.4 Common Fileless/LOTL Techniques and LOLBin Abuse	62

2.5.5 Why Fileless and LOTL Attacks Are Difficult to Detect	71
2.5.6 Implications for Detection Research	72
2.6 Detection Techniques for Fileless and LOTL Attacks.....	74
2.6.1 Event-Based Detection	74
2.6.2 Rule-Based and Signature-Based Approaches	75
2.6.3 Behavioral and Log-Correlation Detection	77
2.6.4 Machine Learning-Based Detection.....	78
2.6.5 Natural Language Processing (NLP) and Semantic-based Detection	80
2.6.6 Statistical and Anomaly Detection Techniques	81
2.6.7 Hybrid and Multi-Stage Detection Systems.....	83
2.6.8 Machine Learning Algorithm Comparison and Selection Rationale	84
2.6.9 Summary of Key Weaknesses in Current Detection Techniques	87
2.6.10 Comparative Review of Existing Fileless and LOTL Detection Frameworks.....	88
2.7 Analytical Models and Limitations.....	93
2.7.1 Graph-Based Analytical Models	93
2.7.2 Semantic-Based Analytical Models	95
2.7.3 Hybrid Behavioral Models.....	96
2.7.4 Statistical and Anomaly-Based Analytical Models.....	98
2.7.5 Explainability and Analyst Trust.....	99
2.8 Evaluation Metrics for Fileless Malware Detection.....	101
2.9 Synthesis and Research Gap	104
2.8.1 Synthesis of Key Insights from the Literature	105
2.8.2 Multi-Dimensional Comparison Matrix.....	106
2.8.3 Discussion of Comparative Literature Findings.....	109
2.8.3 Research Gaps	111
CHAPTER 3 - RESEARCH METHODOLOGY	113

3.1 Research Design Overview	113
3.2 Data Acquisition and Telemetry Sources	116
3.2.1 Sysmon Telemetry.....	117
3.2.2 Windows Management Instrumentation (WMI)	117
3.2.3 Event Tracing for Windows (ETW).....	118
3.2.4 Multi-Source Telemetry Integration.....	118
3.2.5 Relevance to Fileless and LOTL Detection	119
3.3 Telemetry Ingestion and Streaming Pipeline	119
3.3.1 Telemetry Collection Mechanism	121
3.3.2 Streaming and Logical Event Separation	122
3.3.3 Real-Time Constraints and Buffering Strategy	122
3.3.4 Timestamp Preservation and Ordering.....	123
3.3.5 Interface with Downstream Processing.....	123
3.4 Preprocessing and Normalization.....	124
3.4.1 Schema Alignment and Unified Representation	125
3.4.2 Timestamp Normalization and Temporal Alignment	126
3.4.3 Entity Correlation and Contextual Mapping	126
3.4.4 String Normalization and Command Decoding	126
3.4.5 Noise Reduction and Event Filtering	127
3.5 Event Routing and Analytical Branching.....	128
3.5.1 Motivation for Analytical Branching	128
3.5.2 Deterministic Routing Logic.....	129
3.5.3 Contextual Behavior Branch	129
3.5.4 Semantic Command Analysis Branch.....	130
3.5.5 Advantages of the Routing Strategy.....	130
3.6 Contextual Behavior Modeling	131

3.6.1 Contextual Graph Construction.....	131
3.6.2 Feature Representation of Nodes and Edges.....	132
3.6.3 Example of Contextual Feature Computation.....	134
3.6.4 Contextual Anomaly Intuition.....	137
3.6.5 Role of Contextual Modeling in LOTL Detection.....	138
3.7 Semantic Command Analysis	139
3.7.1 Command Extraction and Normalization.....	139
3.7.2 Semantic Embedding Representation.....	141
3.7.3 Example of Semantic Feature Computation.....	142
3.7.4 Role of Semantic Analysis in LOTL Detection	144
3.7.5 Complementarity with Contextual Modeling.....	145
3.8 Hybrid Fusion and Inference.....	146
3.8.1 Fusion of Contextual and Semantic Representations.....	147
3.8.2 Inference and Malicious Probability Estimation.....	150
3.8.3 Decision Thresholding	151
3.8.4 Real-Time Inference Considerations.....	152
3.8.5 Interpretation of Hybrid Decisions.....	153
3.9 Explainable Artificial Intelligence (XAI) Component.....	154
3.9.1 Motivation for Explainability in Fileless Attack Detection	154
3.9.2 Explanation Scope and Granularity.....	155
3.9.3 Example of Explainable Decision Analysis	156
3.9.4 Contextual Contribution Explanation.....	157
3.9.5 Semantic Contribution Explanation	158
3.9.6 Hybrid Explanation Synthesis.....	159
3.9.7 Role of XAI in Model Validation and Evaluation	159
3.10 Detection Time Measurement and Validation Metrics	160

3.10.1 Definition of Detection Time	160
3.10.2 Detection Latency Components	161
3.10.3 Real-Time Detection Constraint.....	161
3.10.4 Validation Metrics.....	161
3.10.5 Relationship Between Detection Time and Accuracy.....	162
3.11 Synthetic Dataset Generation	163
3.11.1 Motivation for Synthetic Data.....	163
3.11.2 Dataset Composition	163
3.11.3 Telemetry Source Coverage	164
3.11.4 Temporal and Behavioral Control.....	164
3.11.5 Dataset Integration into the Research Framework	164
3.12 Summary of Methodology	165
CHAPTER 4 - RESULTS AND ANALYSIS.....	168
4.1 Experimental Setup	168
4.1.1 Experimental Environment	168
4.1.2 Endpoint System Configuration.....	168
4.1.3 Monitoring and Processing Server Configuration.....	169
4.1.4 Network Configuration and Communication Flow	169
4.1.5 Explainability Design.....	171
4.1.6 Software Stack Overview	172
4.1.7 Experimental Scope and Constraints.....	172
4.2 Dataset Description	173
4.2.1 Dataset Overview and Design Principles	173
4.2.2 Dataset Construction and Characteristics.....	174
4.2.3 Benign Activity Dataset	175
4.2.4 Fileless and Living-off-the-Land (LOTL) Attack Dataset.....	177

4.2.5 Dataset Labeling and Ground Truth.....	181
4.2.6 Telemetry Source Distribution.....	185
4.2.7 Dataset Scope and Limitations.....	188
4.3 Detection Performance Evaluation.....	190
4.3.1 Confusion Matrix Analysis	191
4.3.2 Classification Metrics (Precision, Recall, F1, ROC, PR-AUC).....	193
4.3.3 Threshold Sensitivity Analysis.....	197
4.3.4 Risk Score Computation and Interpretation	199
4.4 Comparative Evaluation with Related Works.....	200
4.4.1 Comparison Scope and Evaluation Methodology	200
4.4.2 Offline Detection Performance Comparison.....	202
4.4.3 Real-Time Detection Capability and Latency Comparison	205
4.4.4 Explainability and Analyst Trust Comparison.....	217
4.4.5 Summary of Comparative Findings	221
4.5 Explainability Analysis using SHAP	224
4.6 Summary of Experimental Results.....	225
CHAPTER 5 - RESULT AND DISCUSSION	228
5.1 Conclusions	228
5.2 Research Contributions	230
5.3 Limitations and Threats to Validity	231
5.4 Recommendations and Future Work.....	232
REFERENCES	234
APPENDIX	239
Appendix A. Evaluation and Reproducibility Artifacts	239
A.1 Confusion Matrix (Raw Evaluation Output)	239
A.2 Per-Event Prediction Results.....	239

A.3 Threshold Optimization and Sweep Results	240
A.4 Threshold Sweep Metrics	241
A.5 Reproducibility Statement	241
Appendix B. Case-Based Detection Evidence	242
B.1 Malware Sample 1	242
B.2 Malware Sample 2	243
B.3 Malware Sample 3	246
B.4 Malware Sample 4	248
B.5 Malware Sample 5	250
B.6 Malware Sample 6	252
Appendix C. Detailed LOTL Attack Chain Analysis	254
C.1 Execution → Tool Transfer → Return-to-PS (Staging Chain)	255
C.2 MSHTA Proxy → PowerShell → Cmd Pivot	255
C.3 Regsvr32 Scriptlet Proxy → PowerShell	256
C.4 Rundll32 Indirect Execution (DLL Proxy)	256
C.5 Registry-Based Fileless Container (Store & Read)	257
Appendix D. Supporting Materials	258
D.1 Processed Logs	258
Appendix E – Curriculum Vitae	259
Appendix Summary	261

LIST OF FIGURES

Figure 1.2.1 Root Causes of Detection Challenges for Fileless and LOTL Attacks.....	23
Figure 3.1.1 Architecture of the proposed research framework.....	115
Figure 3.6.1 Example of Contextual Graph Construction from Raw Event Telemetry.....	136
Figure 3.8.1 Context-Semantic Fusion for Real-Time Fileless & LOTL Detection.....	149
Figure 4.1.1 Architecture Communication Flow	169
Figure 4.1.2 Diagram Detailed End-to-End Offline-Online Pipeline	171
Figure 4.2.1 Sample benign activity record used in dataset construction	177
Figure 4.2.2 Sample Fileless and LOTL Attack Event Used in Dataset Construction	178
Figure 4.2.3 Simple Execution Graph from a Fileless LOTL Event.....	179
Figure 4.2.4 Complex Execution Graph (Fileless LOTL Event)	180
Figure 4.2.5 Sample Fileless LOTL Event with MITRE ATT&CK Annotation.....	184
Figure 4.3.1 ROC-AUC Analysis	194
Figure 4.3.2 ROC Curve of the Proposed Fusion Model on the Validation Set	195
Figure 4.4.1 Overall Processing Latency Distribution	210
Figure 4.4.2 Processing Latency Time Series (P50, P95, Min, Max).....	211
Figure 4.4.3 Detection Confidence vs Processing Latency Scatter Plot	211
Figure 4.4.4 XAI Processing Latency Distribution (Overall)	220
Figure 4.5.1 SHAP beeswarm plot illustrating global feature importance	224
Figure A.1 Raw Confusion Matrix Output from Offline Evaluation.....	239

Figure A.2 Illustrates a Sample Per-Event Validation Record from the Prediction Log	240
Figure A.3 Threshold Sweep Results for Decision Threshold Selection	241
Figure B.1 Heuristic detection: PowerShell Execution Policy Bypass Malware 1	242
Figure B.2 Telemetry probes PowerShell (PID/PPID & timestamp) Malware 1	242
Figure B.3 Propose Framework Detection Malware 1	243
Figure B.4 Heuristic detection: PowerShell Execution Policy Bypass Malware 2	244
Figure B.5 Telemetry probes PowerShell (PID/PPID & timestamp) Malware 2	244
Figure B.6 Propose Framework Detection Malware 1	245
Figure B.7 Heuristic detection: PowerShell Execution Policy Bypass Malware 3	246
Figure B.8 Telemetry probes PowerShell (PID/PPID & timestamp) Malware 3	246
Figure B.9 Figure A. 13 Propose Framework Detection Malware 3	247
Figure B.10 Heuristic detection: PowerShell Execution Policy Bypass Malware 4	248
Figure B.11 Telemetry probes PowerShell (PID/PPID & timestamp) Malware 4	248
Figure B.12 Propose Framework Detection Malware 4	249
Figure B.13 Heuristic detection: PowerShell Execution Policy Bypass Malware 5	250
Figure B.14 Telemetry probes PowerShell (PID/PPID & timestamp) Malware 5	250
Figure B.15 Propose Framework Detection Malware 5	251
Figure B.16 Heuristic detection: PowerShell Execution Policy Bypass Malware 6	252
Figure B.17 Telemetry probes PowerShell (PID/PPID & timestamp) Malware 6	252
Figure B.18 Propose Framework Detection Malware 6	253
Figure C.1 List of Sample of malwares	254
Figure C.2 Pseudo-script of a PowerShell attack scenario (MITRE T1059.001 & T1105) ..	255
Figure C.3 Proxy execution pseudo-script using LOLBins (mshta → PowerShell → cmd) ..	255

Figure C.4 Signed binary proxy execution pseudo-script (regsvr32 → PowerShell).....	256
Figure C.5 Indirect execution pseudo-script via rundll32.exe (MITRE T1218.011).....	256
Figure C.6 Fileless attack via registry (PS → reg.exe → PS).....	257
Figure D.1 ML project structure (Data, Training, XAI)	258



LIST OF TABLES

Script Interpreter Abuse (execution)	64
Defense Evasion (Fileless & Obfuscation)	65
Parent-Child Process Abuse.....	66
Discovery & Reconnaissance.....	67
Persistence via LOTL.....	68
Command & Control.....	68
Top 20 Graph Nodes and Edges Associated with LOTL Attacks.....	69
Comparison of Machine Learning Approaches for Fileless Malware Detection.....	86
Detection Technique Comparison for Fileless and LOTL Attacks.....	90
Comparison of Evaluation Metrics Used in Malware Detection	102
Multi-Dimensional Comparison of Fileless and LOTL Detection Frameworks.....	107
Contextual Feature Computation	134
Sample Semantic Feature Vector	143
Example of Feature Fusion	148
Summary of the Proposed Research Methodology	165
Benign Activities Captured in the Dataset	175
Telemetry Source Distribution	187
an overview of the processed dataset	189
Confusion Matrix obtained From Offline Evaluation of the Proposed Model	191

Summary of Validation Performance Across Selected Training Epochs	196
Offline Detection Performance Comparison with Related Works	203
Summary of Real-Time Detection Characteristics and Latency	206
Real-Time Detection & Latency: TEHTRIS EDR vs Framework	215
Explainability Comparison	218
Summary of Experimental Result	226
Threshold Sweep Summary (Excerpt)	241

