SOP

for

Malware Detection Automation System

Prepared by:

IIIT ALLAHABAD TEAM

Team Members:

Swaroop Dora, Piyush Priyadarshi, Avanish Gurjar, Ajay Kumar, Gaurav Singh Painkara

Submitted to:

Punjab National Bank

February 27, 2025

Contents

1 Introduction

1.1 Purpose

This Standard Operating Procedure (SOP) establishes the processes and protocols for operating, maintaining, and updating a malware detection system leveraging machine learning for static and dynamic analysis. The goal is to ensure consistent, reliable threat detection while complying with cybersecurity best practices, including GDPR and ISO 27001. The SOP standardizes procedures, minimizes false positives, and enhances adaptability to emerging threats.

1.2 System Overview

This SOP outlines a structured framework for managing a malware detection system that employs advanced machine learning techniques for:

- Static analysis: Extracting strings, DLLs, and component sizes.
- Dynamic analysis: Monitoring events and file operations in a controlled environment.
- AI-driven detection: Utilizing Network Threat Intelligence (NTI), AI-Powered Static Code Inspection (ASCI), Statistical Threat Profiling (STP), Behavioral Anomaly Detection (BAD), Intelligent Quarantine System (IQS), and Adaptive Threat Learning (ATL).

By implementing these methodologies, the system ensures robust and efficient threat detection through an intuitive, user-friendly interface.

1.3 Scope

This SOP covers the operational, maintenance, and update processes for the malware detection system, including:

- Static analysis (ASCI): Analyzing file structures, strings, and component metadata.
- Dynamic analysis (BAD): Observing program behavior and file operations.
- User interface management: Command Center Dashboard, Real-Time Protection Metrics, and Intelligent User Guidance.

1.4 Definitions

- **Static Analysis**: Non-executive examination of code or files for malicious patterns.
- **Dynamic Analysis**: Real-time behavioral monitoring of executables in a sandbox environment.
- **Machine Learning (ML)**: Algorithms that enhance detection by learning from threat data.
- **Zero-Day Attack**: Exploitation of an unknown vulnerability before patches are available.

1.5 Roles and Responsibilities

- **System Administrators**: Deploy, maintain, and update system infrastructure.
- **ML Engineers**: Develop and refine AI models for ASCI, BAD, NTI, STP, and ATL.
- **Security Analysts**: Monitor the Command Center Dashboard and implement quarantine protocols.
- **UI/UX Designers**: Maintain a responsive design and user-friendly interface.
- **End Users**: Report anomalies and follow cybersecurity guidelines.

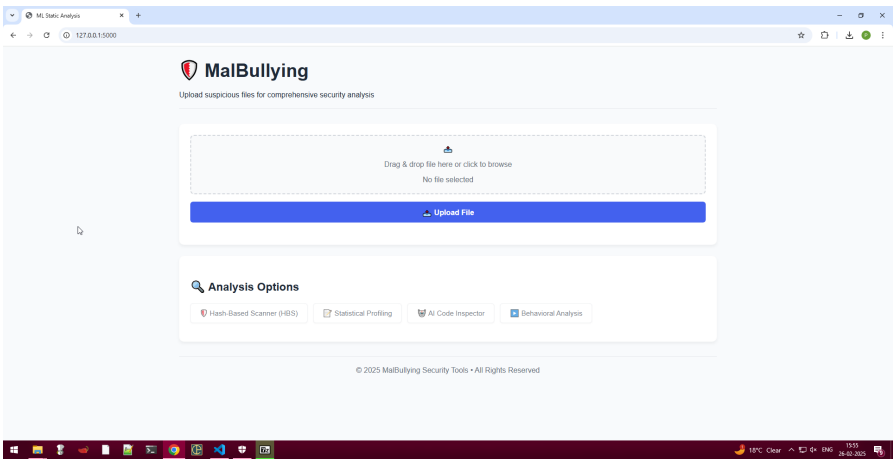

Figure 1.1: Main Interface

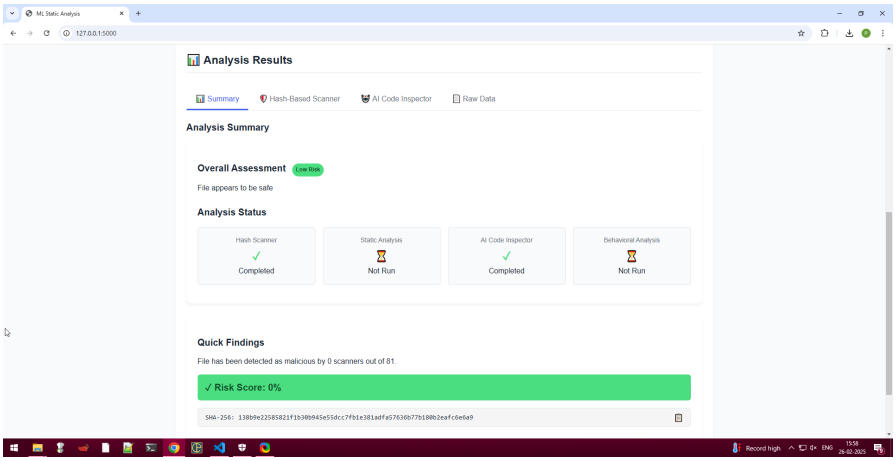

Figure 1.2: Threat Analysis

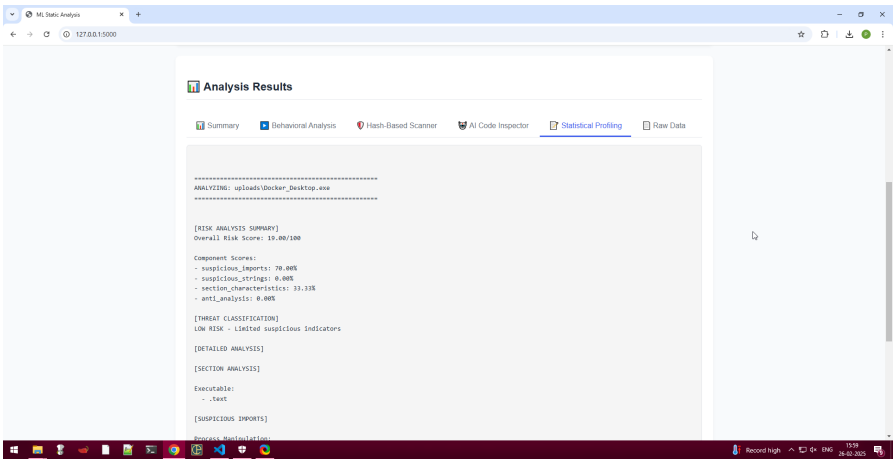

Figure 1.3: Static Analysis

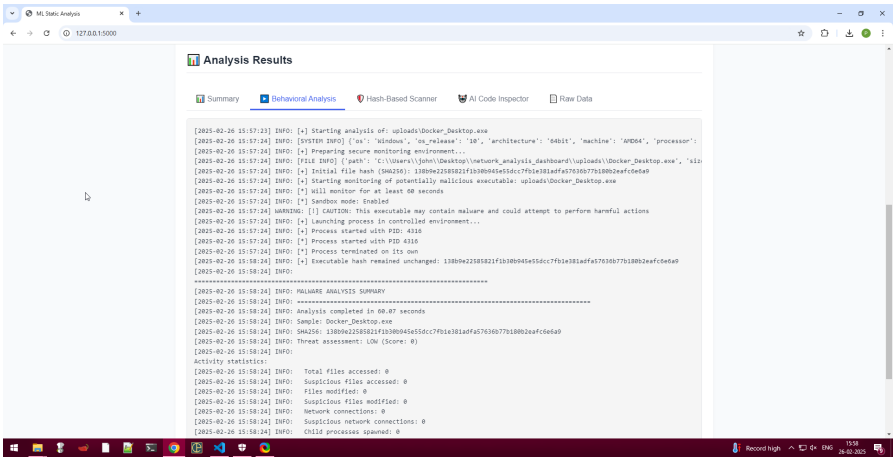

Figure 1.4: Behaviour Analysis

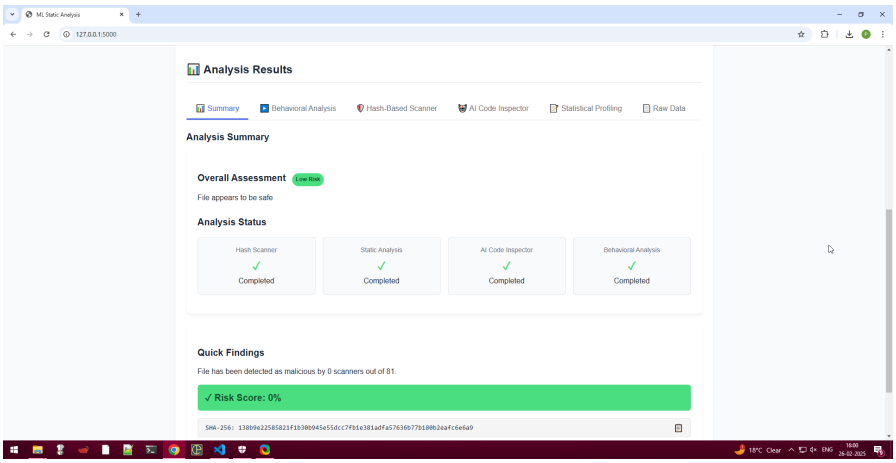

Figure 1.5: Overall Summary

2 Operational Procedure

2.1 Step 1: System Initialization

- Launch the malware detection system and initialize the Command Center Dashboard.
- Ensure synchronization across devices with minimal resource consumption.

2.2 Step 2: Static Analysis (ASCI)

- Upload files for inspection; extract key metadata.
- Apply deep learning models to identify potential malware signatures.
- Escalate suspected zero-day threats to the Intelligent Quarantine System (IQS).

2.3 Step 3: Dynamic Analysis (BAD)

- Execute flagged files in a sandbox environment.
- Monitor program behavior, file operations, and system interactions.
- Log anomalies and feed threat intelligence into ATL for model improvement.

2.4 Step 5: Threat Response and Learning

- Activate IQS for containment and isolation of threats.
- Integrate new threat data into ATL to enhance future detection capabilities.

2.5 Step 6: User Interaction and Reporting

- Update the Command Center Dashboard with real-time threat metrics.
- Provide contextual security guidance and audit logs for compliance.

2.6 Step 7: System Maintenance and Updates

- Regularly update ML models, encryption protocols, and UI components.
- Conduct periodic security reviews to ensure compliance with cybersecurity standards.