CyberShield – Threat Scanner

# Final Project Report

## 1. Introduction

CyberShield is an intelligent desktop application designed to detect and flag potential threats in executable files. Built using Python and PyQt5, this GUI-based malware scanner offers a modern user interface and integrates signature-based, heuristic, and PE-structure-based analysis to assess file safety. It enhances end-user security awareness and assists in quick malware inspection.

## 2. System Overview

CyberShield provides a seamless file-scanning experience with real-time visual feedback. It empowers users to:

- 📁 Select any local file

- 🔍 Perform in-depth malware scans

- 📊 View results and threat summaries

- 🧠 Understand potential threat indicators

Primary Objectives:

- ✅ Threat Detection: Identify known malware signatures and suspicious behaviors.

- 💡 Heuristics: Flag unusually large/small files and abnormal PE imports.

- 👁 Visualization: Display results through a dynamic threat pie chart.

## 3. Technical Architecture

Core Technologies:

- PyQt5: For GUI development (buttons, tabs, progress bar, themes)

- hashlib: For SHA256 signature generation

- pefile: For parsing PE (Portable Executable) structures

- QChart (QtCharts): For visualizing threat levels using pie charts

Threat Detection Layers:

1. Signature-Based Scanning

2. PE Import Analysis

3. Heuristic Checks

## 4. User Interface & Experience (UI/UX)

Design Highlights:

- 🌑 Dark theme with modern fonts and gradients

- 🎛 Tabbed Interface (Scan Results, File Details, Threat Graph)

- 🎨 Stylized Buttons and Effects

Core UI Components:

- File Browser, Start Scan Button, Progress Bar

- Result Viewer, Graph Tab

## 5. Working Process (Behind the Scenes)

1. User selects a file

2. Initial 4KB read for signature & keyword scan

3. PE Header analysis (if .exe/.dll)

4. Heuristic checks for abnormal size

5. Threats are logged and visualized in the chart

## 6. Key Strengths

✔ Multi-layered threat detection

✔ Visual, easy-to-read output

✔ Modern, desktop-friendly interface

✔ No data is uploaded—privacy first

✔ Lightweight and fast scanning

## 7. Limitations & Recommendations

Current Limitations:

- 🚫 No cloud-based threat lookup

- 📦 Threat database is static and local

- ⛔ Only PE files supported (.exe, .dll)

- ⚙ No real-time monitoring

Recommendations for Future Enhancements:

- 🔄 Real-time file system monitoring

- ☁ Cloud-based hash lookup via VirusTotal API

- 🧬 ML-based static analysis for deeper insight

- 📁 Add folder scanning capabilities

- 🌐 Web-based version using FastAPI backend

## 8. Sample Scan Outputs

Clean File:

Starting scan...

Scan completed!

No threats detected.

Malicious File:

🚨 THREAT FOUND: Known malware signature detected!

• Type: Known Malware Signature

• Details: Test MD5 Threat

• Location: File header (SHA256 hash match)

⚠ SUSPICIOUS PATTERN FOUND!

• Type: Suspicious String Pattern

• Pattern: exploit

• Location: Offset 120-127 in first 4KB

## 9. Scan Visualization

The threat graph uses a QPieSeries to visually represent threat ratios. A red slice indicates detected threats, and green signifies a clean scan. Labels include percentage metrics and are interactive.

## 10. Conclusion

CyberShield stands as a robust, lightweight, and intuitive tool for basic static malware analysis. While it does not replace full-featured antivirus solutions, it provides an accessible, privacy-focused interface for identifying suspicious files quickly and effectively.