  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
Synopsis

**Created By:**

* Vibhu Yadav: - 2315300033
* Dushyant Nagal: - 2315300005
* Prem Singh: 2315300018

1. Introduction

**Purpose and Overview: -**

* **Purpose:**

To develop **HORUS (Ransomware Canary Protection System)** — a lightweight, Python-based tool that detects ransomware activity in real time using Windows Event Logs and canary files, and automatically stops malicious processes to prevent data loss

* **Overview:**
  + - HORUS uses special **canary files** placed in the system to detect any unauthorized or suspicious file access.
    - It continuously monitors **Windows Security Event Logs (Event ID 4663)** to catch ransomware activity in real time.
    - Once a malicious process is detected, HORUS **automatically kills the process** and **disables the network** to stop the spread of infection.
    - The system also provides a **simple GUI** for users to initialize protection, monitor status, and view security alerts.
    - HORUS focuses on **fast detection and immediate action**, ensuring minimal data loss during ransomware attacks.

**2. Problem Statement**

Ransomware attacks are growing rapidly and can encrypt thousands of files within minutes. Traditional antivirus programs and signature-based tools often fail to detect these attacks in time. Most existing solutions cannot identify which specific process is responsible for the malicious activity. There is a strong need for a **real-time detection system** that can quickly recognize ransomware behavior, locate the exact process causing the attack, and immediately stop it to prevent further damage.

**3. Proposed Solution**

HORUS provides a **real-time ransomware protection system** that relies on **canary file monitoring** and **Windows Event Log analysis** instead of complex machine learning. The system places decoy (canary) files in sensitive directories and watches for any unauthorized access through **Event ID 4663** logs generated by Windows.

When a suspicious process tries to modify or delete a canary file, HORUS immediately identifies the **Process ID (PID)**, terminates the process, and **disables the network** to stop the attack from spreading.

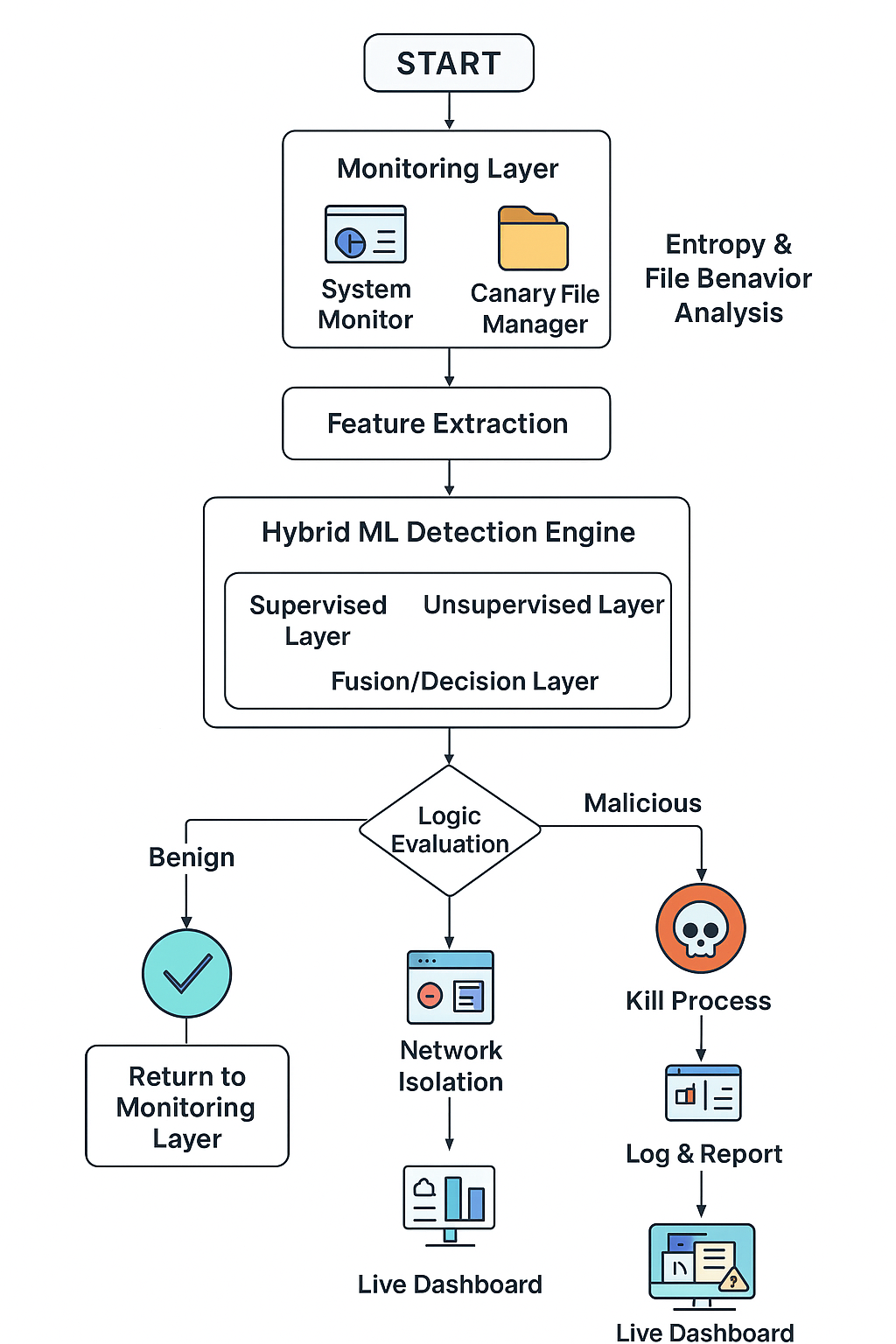
The application features a **simple and user-friendly GUI** that allows users to initialize system protection, start real-time monitoring, and view alerts. All detected incidents are logged for later review and analysis, helping users understand when and how the attack was prevented.

**Addressing the Problem:**

* **Early Detection:** HORUS uses canary files placed in protected directories and monitors Windows Security Event Logs (Event ID 4663) to detect ransomware activity as soon as it begins.
* **Real-Time Monitoring:** The system continuously watches for unauthorized file access or modification attempts by unknown processes.
* **Automated Response**: Once ransomware activity is confirmed, HORUS immediately terminates the malicious process and disables the network to stop further spread.
* **Incident Logging:** All detected events and actions are recorded automatically for later analysis and review.
* **Simple Dashboard:** A Tkinter-based GUI allows users to initialize the system, start protection, and monitor alerts easily.

**Key Goals:**

* Real-time ransomware detection using canary files.
* Identify exact malicious process through Event Logs.
* Automatic process termination and network isolation.
* Log all detected incidents for analysis.
* Simple and user-friendly GUI dashboard.
* Scalable for future security upgrades.

**Flowchart :-**

**4. Key and Innovative Functionality:** **Hybrid Ransomware Detection System**

* **Canary Files:** Uses fake “bait” files to detect ransomware the moment they are accessed or modified.
* **Event Log Monitoring:** Tracks Windows Security Event ID 4663 for file access activities in real time.
* **PID-Based Detection:** Identifies the exact process ID responsible for the attack.
* **Automatic Response:** Instantly kills the malicious process and disables the network to stop infection spread.
* **Process Monitoring:** Continuously watches for suspicious file operations by unknown processes.
* **GUI Dashboard:** Simple interface allows users to initialize, start protection, and view alerts.
* **Incident Logging:** Maintains a detailed log of all detections and actions for later review.

**5. Tools and Technology Required**

* **Programming Language:** Python (core development and automation scripts)
* **Libraries/Frameworks:**
* pywin32 – access Windows APIs and Event Logs
* tkinter – build the GUI dashboard
* os, subprocess, and time – system operations and monitoring
* **Database:** Log files stored locally in structured text or CSV format for easy review
* **Environment:** Windows 10/11 (with Administrator privileges)
* **Operating System Support:**
* **Linux –** primary environment for model development, safe testing, and monitoring**.**
* **Windows –** compatibility testing, since ransomware predominantly targets Windows systems.
* **Testing Tools:**
* **Windows Event Viewer –** to verify Event ID 4663 triggers
* **Task Manager / PowerShell –** for process tracking and validation

**6. Conclusion**

The project presents an effective **real-time ransomware detection and protection system** that uses canary files and Windows Event Log monitoring to identify threats at an early stage.

HORUS focuses on detecting unauthorized file access, identifying the exact malicious process, and **instantly stopping** the attack through **automatic process termination and network isolation**.

It offers a **simple and user-friendly interface**, detailed logging for incident review, and fast response without the need for complex configurations.  
Overall, HORUS provides a **lightweight, practical, and reliable solution** to protect Windows systems from ransomware attacks in real time.