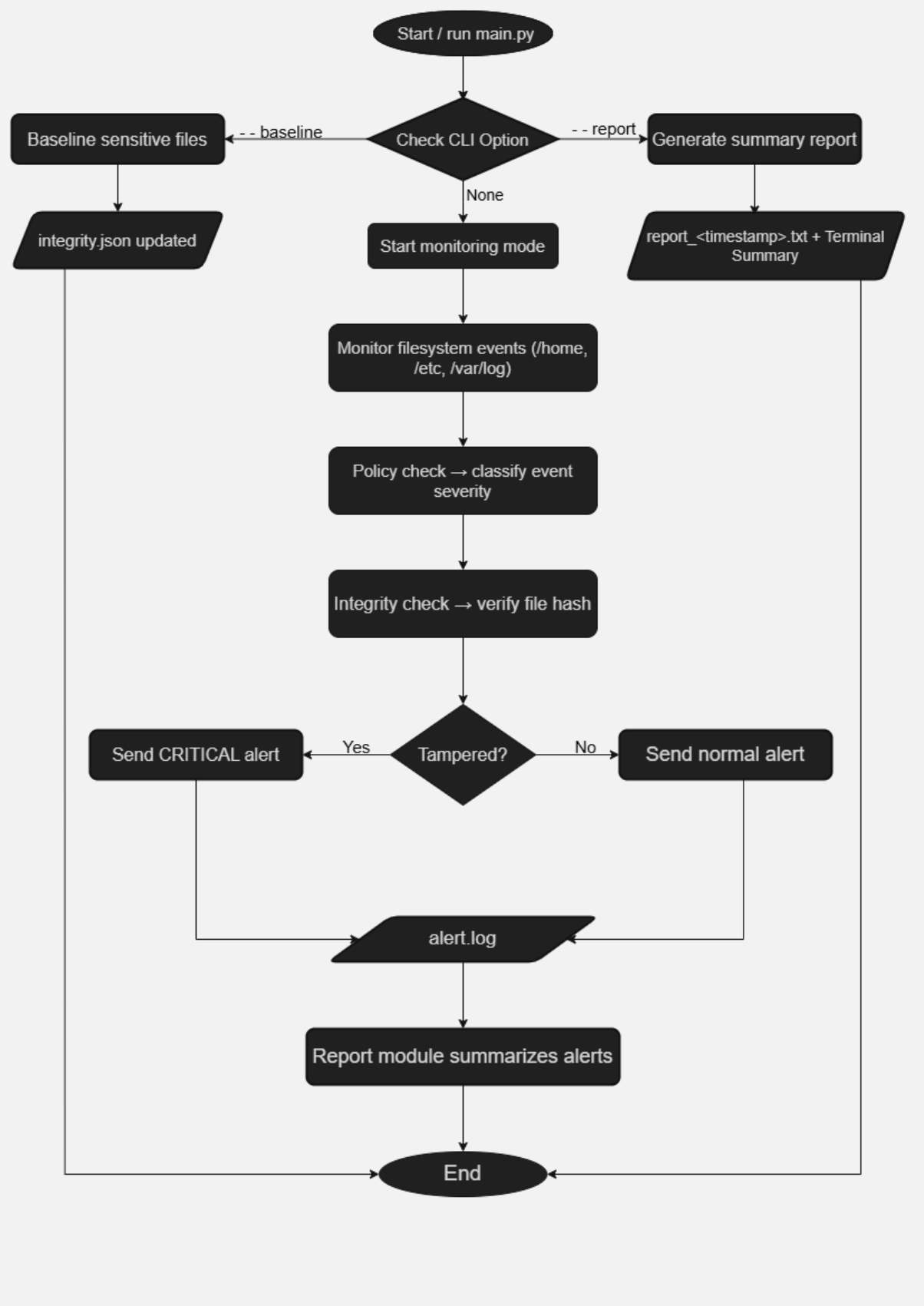
Flowchart - Watchtower: Secure File Transfer Monitoring System



Explanation :

The **Watchtower flowchart** showing how the system runs and what steps it follows to monitor files, check integrity, and create alerts or reports. It works in three main modes based on the command given by the user.

---

1. Start / Run main.py

- The program starts when the main Python file is executed.
- Basic settings and file paths are loaded.

2. Check CLI Option

- The system checks what command the user entered.
- There are three possible paths:
    - **Baseline Mode**
    - **Report Mode**
    - **Monitoring Mode (Default)**

Baseline Mode (--baseline)

Baseline Sensitive Files

- User selects important files or folders to protect.
- The system creates a **SHA-256 hash** (digital fingerprint) for each file.

integrity.json Updated

- These hashes are saved in a file called **integrity.json**.
- This file is later used to check if any file was changed.
- No live monitoring happens here — it is only setup.

Monitoring Mode (Default)

Start Monitoring

- The system begins watching files and folders continuously.

Monitor File System Events

- It tracks actions like:
    - Create file

- Modify file
- Move/Rename file
- Delete file

Policy Check – Classify Severity

- Each action is checked against security rules.
- The system labels the event as **Low, Medium, High, or Critical**.

Integrity Check – Verify Hash

- If a protected file changes, its new hash is compared with the saved hash.

Tampered? (Decision)

- **Yes → Send CRITICAL Alert**
  Means the file may have been changed without permission.
- **No → Send Normal Alert**
  Means the action is safe or expected.

alert.log Entry

- Every alert is saved in **data/alerts.log** with time and severity.

Report Module Summarizes Alerts

- The system can later summarize all alerts into a short report.

Report Mode (--report)

Generate Summary Report

- The system reads the alert log instead of monitoring live files.

Timestamped Report Output

- A report file like **report_<time>.txt** is created.
- It shows number of alerts, severity levels, and important events.

End

- After baseline setup, monitoring stop, or report generation, the program ends.