**Step 5**

**Team Members:**

**Objective:**

The goal of this Step 5 is to develop the detection method that analyzes the monitored (from step 4) system activity and then identifies suspicious behavior that is indicative of the ransomware. We also implement the operational policies and then implements logic to detect the violations that trigger the mitigation.

**Data Source**

We used the monitored data that stored in **monitor.db** (from step 4), which is also logs all the file creation, modification, and deletion events.

These logs data are generated by the monitoring the component implemented in **Step 4** thatusing the Python watchdog library.

**Detection Policy**

**Permitted operations:** Normal file modifications, renaming, or the minor edits.

**Not permitted:** High-frequency of file creation, modification and deletion in a short time window (It’s a common ransomware behavior).

**Defined Policy Rule:**

If it is more than 100 file events (It’s excluding .db/.db-journal files) occur within the 10 seconds and it is flagged as ransomware activity.

**Detection Logic (detect.py)**

* The python script opens the SQLite database and the queries for all the events within the defined time window.
* It also filters out the irrelevant database journal entries.
* If the count of the events exceeds the threshold and then it prints a detection alert.

We used mainly below three for this step

* Python 3
* SQLite3
* datetime module

A computer screen shot of a black screen

Description automatically generated

**This is simulated Ransomware Case:**

In this, Rapid creation of 150 files using a shell loop.

A screenshot of a computer

Description automatically generated

**Output:** which detects from step 4 activity**,** Accurate detection of malicious behavior.

A computer screen with white text

Description automatically generated

**This is Normal Use Case (which is a legitimate User Actions):**

Edited and renamed a file manually from terminal/

A screenshot of a computer

Description automatically generated

Output: "No ransomware detected"

Result: No false positive.

A screen shot of a computer

Description automatically generated