VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

File Integrity Monitoring System

Name: Subramanian Nachiappan

Regno: 20BCE1019

PBL1: Title Finalization with Objectives

Under the Guidance of

Dr.Subbulakshmi T

Title Finalization with Objectives

Title: **File Integrity Monitoring System**

Finalizing the title and objectives plays a very important role for making a project successful. The title should accurately reflect the purpose of the system while being concise and easy to understand.

We have decided to term the title as “File Integrity Monitoring system” as it is the most commonly used and widely recognized in the industry, making it appropriate and straightforward title

Reasons for finalizing the title are:-

1. **Clear and Concise**

   The title "File Integrity Monitoring System" is clear and concise, making it easy to understand and remember. It accurately describes the system's main function, which is to monitor files for any unauthorized modifications or changes.

2. **Industry Standard**

   "File Integrity Monitoring System" is a widely recognized and commonly used term in the cybersecurity industry. By using this standard term, it can help to ensure that the system is easily recognizable and understood by IT professionals and security experts**.**

3. **Reflects Purpose**

   The title reflects the purpose of the system, which is to ensure the integrity of files. It conveys the idea that the system is designed to monitor files to ensure that they have not been modified or tampered with, which is critical for maintaining the security and integrity of an organization's data.

4. **Consistency**

   Using a consistent title can help to avoid confusion and ensure that everyone within the organization is using the same terminology to refer to the system. This can help to promote better communication and collaboration between different teams within the organization.

In summary, "File Integrity Monitoring System" is a suitable title for a system designed to monitor files for unauthorized changes or modifications. It is clear, concise, industry-standard, reflects the system's purpose, and promotes consistency and effective communication within an organization.

Objectives Of Project

1. **Detect the File Modifications**

The primary objective of the project is to develop a file integrity monitoring system that can check the integrity of a directory and the files in it. The system should use a hashing mechanism to compare files and determine if any files have been added, modified or deleted.

2. **Suspicion Detection**

It also should incorporate suspicious hash checks only for the files which has been added or modified by passing the hashes of the file to the VirusTotal API and using PE File Modules for executable files to detect any malicious activity. The changes made you should be flagged whether it is suspicious or not.

3. **Generate a Log File**

The system should generate a log file of the directory of interest containing four comma-separated values: file name, status, time, and suspicion check. This log file will help user to track changes made to files in the directory and detect any suspicious activity.

4. **Support Manual Log Analysis**

The system should allow for manual log analysis using a regex-based filter to acquire relevant log data. This should help the user to find the log changes between given period of time, types of file change and even filter it using the name of file. This feature will help user to easily identify suspicious activity and investigate security incidents.

5. **Enable Log Data Export**

The system should allow users to export selected log data and receive it via email. This will enable user to easily share relevant information with other members or organization and ensure that critical information is communicated quickly and efficiently.

Overall, the objectives of the project should be focused on developing a file integrity monitoring system that should detect changes in the file and log the changes ,detect suspicious activity, support manual log analysis, and enabling the using to export Log Data via email. The system should be designed to meet compliance requirements and enable user to respond quickly and effectively to any security incidents.