Integrity Plus

A Project By :

Kishore Kumar.A
S.R.Aryaan Malik
Vijay Akash.R

Supervisor
Mrs.Nivitha.J

Abstract

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is actively engaged in helping organizations address the challenge of ransomware and other data integrity events through the Data Integrity projects. These projects help organizations implement technical capabilities that address data integrity issues. The objective of this document is to provide an overview of these Data Integrity projects; provide a high-level explanation of the architecture and capabilities; and explain how these projects can be brought together into one comprehensive data integrity solution.

Literature Survey

Reference : Data Integrity identifying, Monitoring and protecting assets against Virus and Ransomware. (By : The MITRE Corporation , October 1, 2020)

Integrity is part of the CIA security triad which encompasses Confidentiality, Integrity, and Availability. As the CIA triad is applied to data security, data integrity is defined as “the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.” An attack against data integrity can cause corruption, modification, and / or destruction of the data which ultimately results in a loss in trust in the data. This document provides an overview of these Data Integrity projects; providing a high-level explanation of the architecture and capabilities, and how these projects can be brought together into one comprehensive data integrity solution. This comprehensive data integrity solution can then be integrated into a larger security picture to address all of an organization’s data security needs.

Existing System

- Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events addresses data integrity before a potential attack. It details the need for a thorough knowledge of the assets within the enterprise and the protection of these assets against the threat of data corruption and destruction. This project proposes an architecture with multiple systems that work together to identify and protect an organization's assets against the threat of corruption, modification, and destruction.

- The Integrity Monitoring capability establishes baselines of files and systems, which is essential in determining information about any integrity changes that occur to the data within those files and systems. At the same time, the Backup capabilities allow components within the enterprise to produce backup files of data. Some stored data, including backup files, may benefit from a Secure Storage capability. Secure Storage allows data storage with additional data protection measures, such as write once read many technologies.

Proposed System

- This Project is aimed and focused to satisfy the CIA triad when it is been performed. It is completely carried out using "Windows Powershell" which makes it easier to trust and execute the project as Powershell is a default program in Windows based system. Malware and Ransomware analysis is done through open source tools on a "Hash" based verification

- The project is created using "Powershell ISE" which is used to create scripts that automates the process of integrity monitoring and alert generation. The scripts that are created can only be executed either by using administrative privilege or a separate username and password is created for accessing and executing the scripts. VirusTotal is the open source tool to verify Malwares and Ransomwares using unique "Hash" generated for every file.

- Separate aliases and environment variables are created which makes it easy to access ,monitor and maintain integrity in any directory location.

Tools Used

Hardware :

Any computer / machine that is capable of running windows 10 / 11 / Windows Server above 2008 and Python 3.7

Software:

- Windows 11 / 10 / Windows Server (above 2008)
- Python 3.7 or higher
- Powershell ISE
- VirusTotal
- Powershell Objects (Get-FileHash, Custom Scripts etc.)

Execution:

Any directory with large quantity in Files and folders at any desired file location to monitor Integrity and to find Malwares.