CorreLog File Integrity Monitor

Our File Integrity Monitor (FIM) agent scans files on your Windows and UNIX systems, periodically checking for unauthorized changes, and automatically issuing alerts when files are added, deleted, or modified. This interoperable agent works with all Syslog capable managers, and has specific remote configuration functions that work with CorreLog to provide proactive system security.

Overview

The CorreLog FIM is designed to support enterprise security requirements with special regard to PCI/DSS (as well as other) security guidelines. This simple to use program also has direct application in performance management (such as with regard to monitoring Windows Prefetch files) as well as asset and configuration management.

The CorreLog FIM can be deployed in both highly centralized or decentralized environments, as well as a combination of both, thus providing maximum flexibility to address enterprise security requirements and architectures.

The File Integrity Monitor executes as a stand-alone process on Windows 32-bit and / or 64-bit platform, as well as a wide variety of popular UNIX platforms. Periodically (by default each hour) this process scans all the files on the system as specified by its configuration file. If any file has been added, deleted, or modified, the file name is recorded and a Syslog message is sent to the main CorreLog Server. At the CorreLog Server, the operator can create (or recreate) a file image, can inspect the list of changed files, and can set FIM parameters.

The program is easy to install and use, and contains the following specific features and functions.

- **Fast File Scans.** The File Integrity Monitor is designed to monitor large numbers of files quickly and non-intrusively. The program will typically scan 10,000 files within one or two minutes, permitting hourly checks of file integrity, recording file additions, deletions, and / or changes.
- **Ability To Monitor Files By Directory.** The File Integrity Monitor is easy to configure, and allows the user to specify files by directory, including the ability to match and exclude files by directory name, file suffix, file prefix, or other keywords. This allows an operator to precisely target special files on the managed system.

- **Ability To Perform File Checksums.** The File Integrity Monitor checks the file creation time, modify time, and file size to determine whether a file has been modified on the system. As an additional feature, the user can enable the calculation of checksums on each file to check whether any single bit in the file has been changed.

- **Ability To Tune CPU Usage.** The File Integrity Monitor allows the user to throttle the amount of CPU used by the process, as well as schedule the execution hourly, or daily. This permits the system to operate non-intrusively on a variety of different platforms, including highly loaded systems.

- **Remote Configuration Capabilities.** The File Integrity Monitor allows the user to remotely access and adjust (with authentication) the program configuration data, permitting the user to make changes to the file integrity monitor while it is running. Additionally, the user can obtain real-time status from the File Integrity Monitor, to view the remote status and state of the program.

- **Support for 64 Bit Platforms.** The File Integrity Monitor supports both 32-bit and 64-bit platform architectures. On 64-bit systems, the File Integrity Monitor can access system pathnames that are not accessible to 32-bit programs.

FIM Applications

In addition to monitoring the integrity of system executables and configuration files (to detect tampering), the File Integrity Monitor provides various other specialized functions that extend its role to include asset, configuration, and performance management.

- Windows Update Monitor The FIM agent is highly useful in detecting when automatic Windows updates occur, or when software is automatically upgraded to new versions. The success or failure of an update process is easily detected with a single correlation rule that spans the entire enterprise, or divisions thereof.

- Windows / UNIX File Inventory The FIM agent creates an image file of specified directories, permitting a CorreLog user to easily inspect the contents of monitored directories, including the ability to search for certain common files (or their absence.) This includes the ability to remote fetch file listings from machines (with authentication.)

- Windows File Prefetch Monitor The FIM agent can continuously monitor the Windows "Prefetch" folder to determine what programs are commonly accessed on the computer system, such as screensavers, licensed software, or unauthorized programs. As new programs are executed, CorreLog leverages the Prefetch functions of XP, Vista, Windows 2008 and Windows 7 to record user activity, and detect what programs are being used on the network.

- PCI-DSS Compliance The FIM agent satisfies file monitoring of the PCI DSS specification, which requires a file scan to be run on a weekly basis. The agent provides provable evidence to auditors that you are in compliance with this aspect of PCI-DSS, and protects your customers against unauthorized changes to files that might compromise their sensitive data.

Contact us now to arrange a demo - info@agileise.com or call +44-1582-380140