Elimination of False Positives

Synopsis:

FIM+ improves z/OS security by detecting malicious alterations of sensitive datasets and infrastructure components. FIM+ accomplishes this, without extra effort, by automatically capturing the changes to the trusted state as they flow through the change process.

By adding a single step to your implementation process, you can make changes during an approved window, but not generate unneeded alerts that require investigation.

How do we do this? FIM+ supports a lock / unlock capability and FIM+ simply:

1) Unlocks the set of monitored files
2) Learns Updates
3) Locks the monitored files

Having learned about the approved updates, FIM+ can then detect unapproved alterations, like malware programs, time bombs or access backdoors, on an ongoing basis and alert you when any are found.

We typically recommend a phased implementation. This allows FIM+ to be installed in a few hours, protecting your most important services, yet enabling future expansion. This approach has been used in other customer sites moving to improved security in a step-by-step fashion.

No false positives, no unneeded investigations, more thorough security. Simple and Quick

What FIM+ Does:

FIM+ was built to scan your trusted infrastructure, systems and applications programs, parameters, JCL, and other components, to ensure that no malware has been imbedded by external or internal perpetrators. FIM+ will not report false positives because it identifies everything that is allowed in an environment—and reports any variances on that trusted state.

FIM+ does this by scanning all components immediately after they have completed quality assurance or rigorous testing (the trusted baseline). The FIM+ scan process creates a baseline set of hash keys and stores these in an encrypted dataset. Subsequent scans of your production system create an up to the minute set of keys, which are then compared to the trusted baseline in the vault. If the keys match all is good and no discrepancies are reported.

A plug-in step allows FIM+ to capture approved changes automatically and to revise the baseline keys correspondingly. This process creates NO False Positives. If FIM+ reports a problem, there has been a modification that has bypassed your normal processes and should be reported.

Routine Maintenance / New Software Versions?

FIM+ deals with that automatically. As the final step in your acceptance process, you simply have FIM+ create a new baseline. Let's call that V2.5. The previous version, V2.4 is still running in production on 14 LPARS. FIM+ continues to check them against baseline V2.4, business as usual. When the deploy date arrives you use the standard deployment process, but you add one step at the end that tells FIM+ that the new V2.5 is running in LPAR 1 (but no change to LPARs 2 – 14). You run a FIM+ scan immediately on LPAR 1 and, unless there was some type of problem with the deploy, everything checks out fine. No False Positives, and confirmation the deploy was completed correctly. As other partitions are upgraded, one step tells FIM+ to move on to scanning that LPAR against the V2.5 baseline. If there is a problem you simply back out, with the last step telling FIM+ to revert to scanning using the V2.4 baseline. An FIM+ scan confirms (or not) that the back out worked properly. Again, no false positives and total confirmation.

Other implementation options: FIM+ was designed to run as an integral part of your DevOps tool chain. Using standard REST APIs, FIM+ can interoperate with your mainframe and Open Systems or Cloud based tools. FIM+ has several models of implementation serving the needs of a varied customer environments. Please contact MainTegrity to discuss specific needs and implementation options.