FIM+ V2.2 Early Warning Package

MainTegrity FIM+ enhances its industry-leading cyber security and resiliency capabilities with the release of Version 2.2 with planned delivery in September 2023. In addition to the superior detection and recovery built into the existing product, V2.2 will include our Early Warning package (FIM+ EW).

FIM+ EW will provide continuous monitoring of active datasets and files to identify suspicious activity, often before a cyber-attack occurs. EW also provide real-time monitoring for unusual user behavior, atypical access, and unexpected use of encryption services.

Existing alerts and other corrective actions can then be initiated automatically, avoiding, or minimizing malicious damage. This package complements existing FIM+ functionality, making it effective against ransomware, data exfiltration and other types of attacks on z/OS mainframes.

FIM+ EW features include:

- **Continuous Dataset Monitoring** – FIM+ EW will monitor active data files and libraries for unusual actions even if they are not included in regular FIM+ validation scans. The datasets can be selected by high-level qualifier or specific dataset name and may include VSAM, sequential, PDS/E, and USS file formats.

- **Behavioral Analytics** – During the early stages of modern attacks, perpetrators often need to look at data and programs that are not a part of their normal working pattern. This is called the reconnaissance phase. FIM+ EW will detect unusually high access rates or access patterns that are characteristic of this behavior. Specifically, the product will detect snooping by monitoring user read accesses to configuration datasets (PARMLIBs, PROCLIBs, VTAMLST, TCPPARMS, etc.), authorized datasets and other files. Accesses are collected for an interval, and if they exceed customer-defined historical trends, an alert or other action can be triggered.

- **Malicious Encryption Attacks** – All modern mainframes are capable of encryption at blistering speed. This provides advanced defensive capabilities, but can also be weaponized in the hands of unscrupulous criminals or rogue state entities. Many CISOs are worried, rightfully, that IT systems are vulnerable to catastrophic data encryption events, the root cause of many ransomware attacks.

  Conventional approaches attempt to determine that files have been encrypted, but this often occurs long after the data has been compromised. FIM+ EW will continuously monitor for malicious use of encryption services. Automated actions, such as suspending or cancelling the offending process, can then be taken, limiting damage to a few seconds, rather than the hours or days it may take to recognize and halt the attack with existing tools.

- **Mass Delete Detection –** Attacks on mainframes may include the deletion of a large numbers of datasets in order to cripple ongoing operations. To address this, FIM+ has been enhanced to be vigilant for batch jobs or TSO users where the delete count exceeds a customer-defined threshold.

- **Mass Dataset Updates –** Attacks may involve overwriting existing datasets. FIM+ EW will monitor dataset update activity. If the number of datasets updated exceeds a customer defined threshold, an alert is raised, and corrective action enabled.

- **Mass Dataset Scanning -** Attacks may involve reading through datasets in search of sensitive data. FIM+ EW will monitor dataset read activity, and if it exceeds a customer-defined threshold, an alert is raised.

All functions minimize administrative effort with built-in processes to collect relevant information, use of approved lists to minimize false positives and learning capabilities to capture site-specific approved usage patterns.

FIM+ 2.2 also serves as an integration point, enabling seamless interoperability with other tools. This delivers a comprehensive solution for protection, detection, response, and recovery. By utilizing FIM+, customers can achieve exceptional cyber security and resilience, built on the foundational controls and best practices of Zero Trust.

Compliance with international security standards, such as PCI DSS, NIST Cybersecurity Framework, Financial Services Cyber Resiliency Guideline, and many others, is also provided.