VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Software Application Monitoring and Malware Detection (SAMM)

SAMM Overview

What is SAMM?

1. SAMM is a discovery tool for software assets installed on System Z, it discovers all software products installed via SMP/E & performs File Integrity Monitoring (FIM) for system assets running on System Z.

2. SAMM uniquely compares LMODs contained in datasets on a system to the LMODs created by SMP/E and determine if the LMOD running on a system came from and is therefore a valid version of that LMOD via SMP/E. This is malware detection in that any LMOD or module modified that comes from an unknown source is detected and alerted upon by SAMM.

3. SAMM is by definition a continuous monitoring system as required by compliance regulations. It monitors all components of the operating system and vendor software, as well as validates that any changes made are correct and valid.

4. SAMM is the only reporting tool that can identify the existence of a specific PTF or APAR on a system without the CSI's existing on that given system. SAMM can answer the question, "Is the following PTF/APAR applied to and running on a particular system or set of systems?". It does not report on APPLIED PTFs/APARs, it reports on the existence of the PTF/APAR in the libraries running on a system.

5. SAMM will automatically enumerate, plus baseline & then detect changes to APF, LPA, LINKLST, System Parmlibs, System Proclibs, Steplibs and Joblibs from Started Tasks, TSO users and Batch Jobs without any human interaction or intervention.

6. SAMM monitors for additions and deletions to APF, LPA, LNKLST and will adjust the datasets that are being monitoring as those changes occur while alerting to the fact that the change did occur and checking those changes against the system of record like SAMM does for all modifications.

7. SAMM will detect changes to any of the monitored Datasets, regardless of whether the change was made on the system that SAMM is monitoring. SAMM uses MLT processing, SMF records, baselined attributes along with STOW and DSERV exits to ensure complete and accurate monitoring of System Z.

8. SAMM includes automated processing to backup the Master Files of data it uses to store information as well as automatic reorganization of files after the backups occur. This is controlled by settings specified by the installation.

9. SAMM utilizes Vanguard Active Alerts to send and process alerts and to deliver those alerts optionally to a SIEM.
10. SAMM includes both a feature rich Web UI and a 3270 interface for interaction with users. All SAMM software will run within the system Z environment. Also, SAMM uses ZIIP processing for Message Digest creation to reduce CPU overhead if available.

What is a FIM product?

FIM products perform monitoring of files and record activity against those files usually through the use of baselined attributes of the files and then reporting on changes to those attributes.

Why does an organization need SAMM?

SAMM is not only a compliance product, it is also a security intelligence product.

1. The easiest way to discover an attack on your system, whether it be a bad actor attempting something nefarious, or simply a mistake (from both internal and external threats), is to monitor the state of your system continuously. This includes that state of the executables and configuration files that make up your Operating System Environment and alerting when changes occur. The problem is that changes occur all the time and somehow intelligence needs to be inserted into this process so that a determination can be made as to the validity of the change(s) observed.

2. SAMM not only monitors the state of the executable and configuration files that make up your Operating System but it categorizes those changes it observes. It provides intelligence about the changes being made. Without SAMM, an organization is going to struggle with knowing what changed and when it changed. Additionally, an organization without SAMM working to determine if the change was a valid change is nearly impossible. Change control is one method people use to attempt this, but change control is a self-attestation in that the actual changes cannot be verified against the original source of the record.

3. SAMM has a unique feature that is not found (to our knowledge) in any other software product today. SAMM can determine if the module that was modified came from your record of source (SMP/E) and what version of that module it represents, and does so on a continuous basis. SAMM will determine if a change that was introduced into the operating system or configuration files is a KNOWN change. (I.E. it matches the LMODs or some permeation of that LMOD from your SMP/E environments set of known executable modules) and is therefore a KNOWN and valid executable module, or alternatively that the change that occurred at least matches back to the last version of the module as observed by SAMM. It does this automatically without human intervention on an ongoing basis.

4. This type of monitoring is required by nearly every compliance regulation that organizations are required to deploy, including, but not limited to, SOX, PCI DSS 4.0, DORA, NIST, HIPAA, GLBA, NYC500 and a plethora of others. Following are some examples:

SOX Section 302: Corporate Responsibility for Financial Reports

It is required that the CEO and CFO certify the accuracy of financial reports and the effectiveness of internal controls. It requires companies to maintain accurate and trustworthy financial reports.

By identifying unauthorized or unexpected modifications to crucial files and configurations, FIM contributes to the protection of financial data integrity. This helps businesses comply with section 302 of SOX.

PCI 4.0 section 11.5.2 states that an organization must:

Deploy a change-detection monitoring (such as file integrity monitoring) to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least once per week.

This is *exactly* what SAMM does, but SAMM goes even further by informing the installation of the validity of the change by matching it back to the system of record (SMP/E).

HIPAA (Health Insurance Portability and Accountability Act)

Mandates security measures to protect electronic health records, including monitoring file integrity.

Section 164.312(c)(1) of HIPAA requires covered entities to implement policies and procedures to protect ePHI from improper alteration or destruction.

Section 164.308(a)(5)(ii)(C) involves implementing procedures for monitoring login attempts and reporting discrepancies.

Section 164.308(a)(6)(ii) requires procedures for identifying and responding to security incidents, including mitigating harmful effects and documenting the incidents and their outcomes.

SAMM provides data integrity and further helps ensure that patient information is correct and dependable by quickly identifying and offering real-time alerts and audit logs of file changes for any unauthorized or unexpected modifications to important files, directories, and configurations.

NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

FIM is included as a recommended control within the publication. Specifically, FIM falls under the category of System and Communications Protection and the control SI-7: software, firmware, and information integrity.

NIST Cyber Security Framework version 1.1 and 2.0

The NIST Cyber Security Framework requires that organizations follow 5 steps: identify, protect, detect, respond and recover during and from a cyber security event.

SAMM aids with all steps of the Cyber Security Framework it identifies with application's on z/OS, and protects and detects changes to those software applications by ensuring that modifications made are detected and validated. SAMM helps and assists in the recovery process by ensuring that the assets modified are from a known and valid source (SMP/E) which in itself is an aid to recovery. If you are unsure of the state of your modules at any given point in time, how can you recover to a known and valid backup point?

ISO 27001 A. 12.4. 1: The mandate requires organizations to implement appropriate controls to detect unauthorized changes to critical files and folders

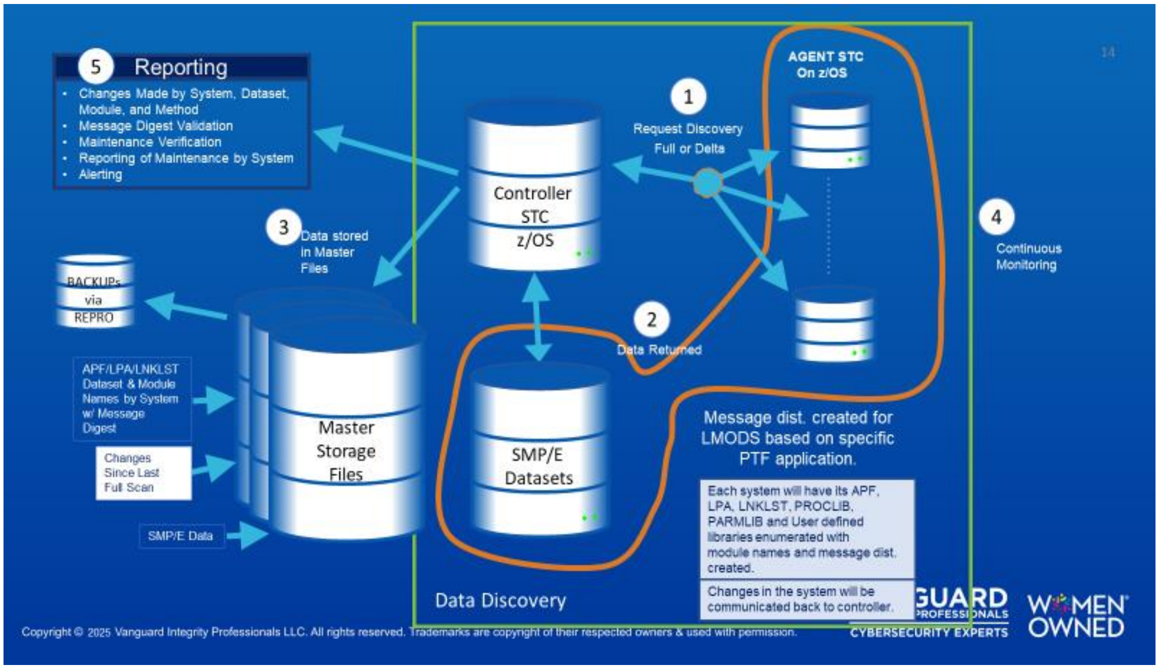
SAMM by definition not only detects changes to critical files and datasets but it can determine if the change made is a valid change regardless of the authority used to make the change.

Event Logging report is related to event logs recording user activities, exceptions, faults and information security events that shall be produced, kept, and regularly reviewed. **SOX** (Sarbanes-Oxley Act) – Focuses on financial data integrity, where FIM can help ensure compliance.

GPDR - Article 51 (f) of the GDPR mandates organizations to prevent unauthorized processing

For this, they need to set up security configurations and monitor the changes to these configurations to detect unauthorized access and processes. Organizations also need to audit all the operations performed on personal data to ensure the processes are carried out in a legitimate manner.

SAMM provides both monitoring of executable files as well as security and operational configuration files. For enhanced security authorization checking and validation, Vanguard Enforcer and Policy Manager are recommended.



5 Reporting

- Changes Made by System, Dataset, Module, and Method
- Message Digest Validation
- Maintenance Verification
- Reporting of Maintenance by System
- Alerting

3 Data stored in Master Files

BACKUPs via REPRO

APF/LPA/LNKLST Dataset & Module Names by System w/ Message Digest

Changes Since Last Full Scan

SMP/E Data

Master Storage Files

Controller STC z/OS

SMP/E Datasets

1 Request Discovery Full or Delta

2 Data Returned

AGENT STC On z/OS

4 Continuous Monitoring

Message dist. created for LMODS based on specific PTF application.

Each system will have its APF, LPA, LNKLST, PROCLIB, PARMLIB and User defined libraries enumerated with module names and message dist. created.

Changes in the system will be communicated back to controller.

Data Discovery

14