MAINTEGRITY

New Ways to Maintain Integrity

Stop, Thief!

FIM+ Intrusion Detection for Z

Partners:

SDS

IBM Registered Business Partner

splunk>

Presented By: Al Saurette (403) 818-8625 al@maintegrity.com

Brandon Saurette (587) 897-7502 brandon@maintegrity.com

In the next 40 Minutes we will

Prove FIM+ is the Only z/OS product that can:

- Deliver OnDemand verification that software levels are correct – or not
- Provide absolute proof of compliance with PCI, NIST and data standards
- Get through your next audit in ½ the time
- Synchronize multiple LPARs and applications
- Verify approved changes are correct before the Monday blues
- Fix known integrity exposures such as SMP/E injection
- Detect internal attacks rigorously
- Eliminate False Positives in other products

Start saving your time and money

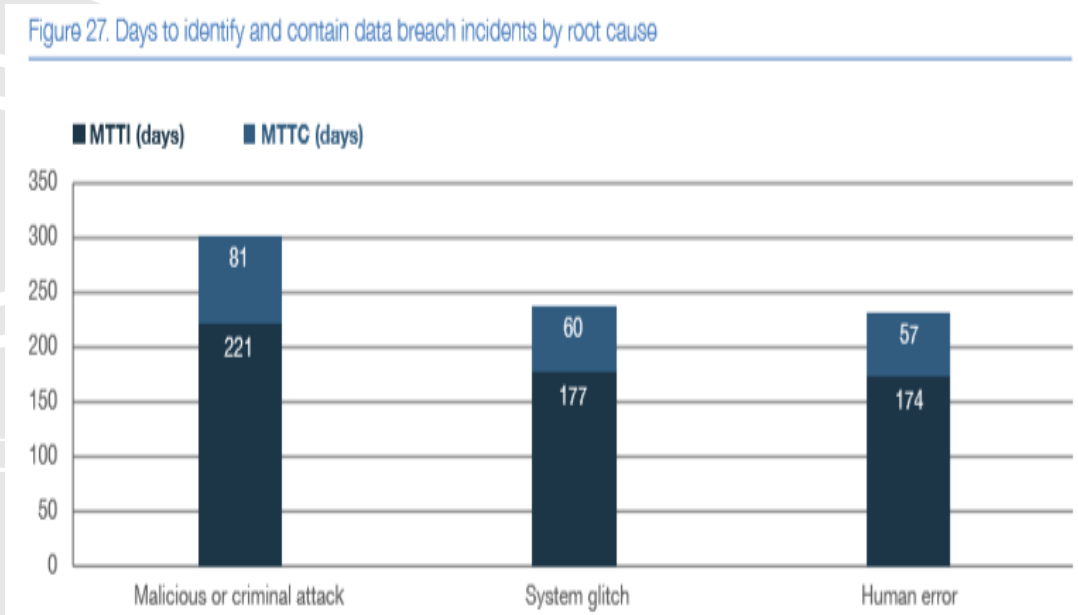
Business Risk – July 2018

IBM / Ponemon report

- Surveyed 477 organizations
- Mean time to identify a breach – **197 days**
- Mean time to contain a breach – **+69 days**

Why you should Care

- USA Average cost: $7.91 Million
- Unquantifiable brand and reputational impact
- You may lose your job



IBM sponsored 2018 Ponemon *Cost of Data Breach Study* https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

What Does FIM+ Do?

File Integrity Monitoring

- Create an application or file baseline key from a trusted source
- Save the multi-level hash keys in an encrypted vault
- Later scan files / programs in use to detect mismatches

Only FIM can prove components are correct

- Executable / source programs, JCL, config members, panels
- Sequential, encrypted and Log files
- USS / HSF, Shell scripts, Java, binaries, html, etc

Integrates with SIEM (Splunk, QRadar, etcl)

- Alerts sent to SIEM for standard escalation
- Focus incident response - exact components / interval

Delivers Blistering Performance

What Can FIM+ Do That Others Can't?

OnDemand Integrity Validation

Bit by bit clarity that components match desired state
Provide conclusive Audit – Code, configs in use are right
Give management a clear answer and get back to work faster

Improve Existing Intrusion Detection:

Detect internal & external attacks conclusively (stolen credentials)
Identify all altered, added and deleted modules
Fix known integrity exposures that currently have no defense

Compliance:

FIM required for new PCI, NIST standards
Success records prove that software levels are correct
Save real $$$ by reducing the time & effort spent on audits
ITIL – Security planning, Root cause analysis

Compliance

PCI DSS (3.2)

- ✓ 10.5 – "**Use file-integrity monitoring** or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)."
- ✓ 11.5 – "Deploy a change-detection mechanism (i.e. **file-integrity monitoring** tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons **at least weekly**."

NIST

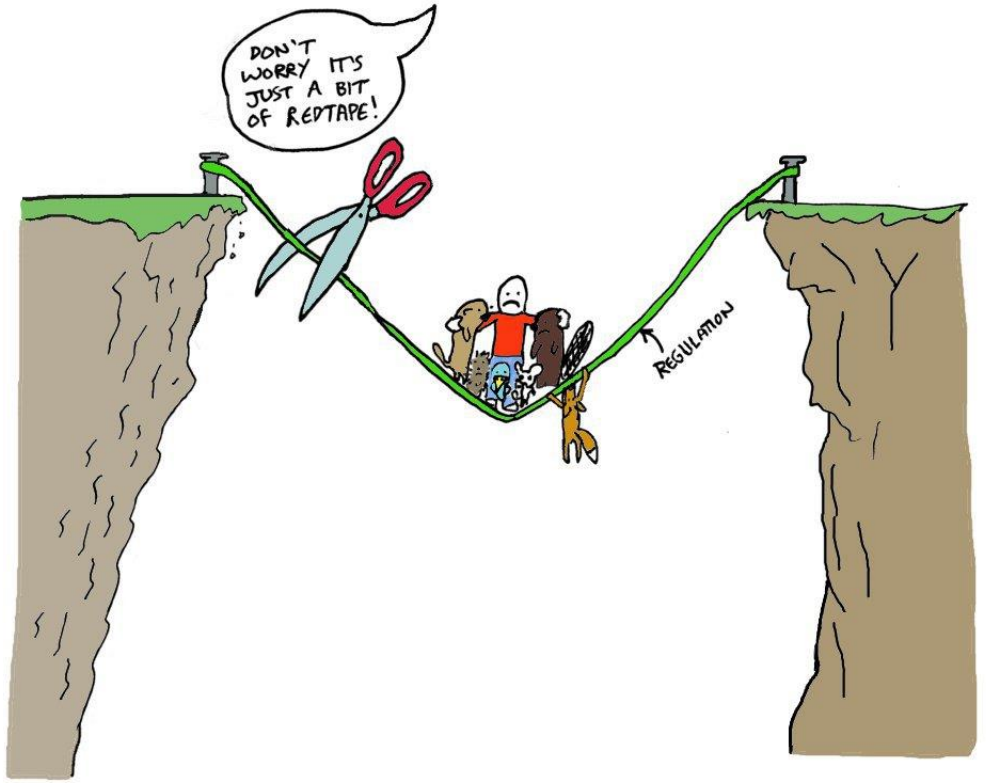
- ✓ SP 800-53 (FISMA): Control SI-7 "the organization **employs integrity verification** tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]."
- ✓ SP 800-66 (HIPAA): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

FIPS-140

- ✓ A cryptographic module shall perform the following power-up tests: cryptographic algorithm test, **software/firmware integrity test**, and critical functions test

GDPR

- ✓ Article 32 – Security of Processing
  - (b) "ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
  - (d) process for **regularly testing, assessing and evaluating** effectiveness of technical and organizational measures



Regulation protects the things we care about - we need to keep it that way

@CARTOONRALPH

Other Problems FIM+ Helps

System Sync:

Confirm all system LPARs & application groups match desired config
Enable faster disaster recovery tests, data center consolidation
Handle system specific files (different but unchanged)

Production Drift:

Master/QA diverges from production image(s)
Emergency changes – authorized circumvention of process
Retroactive correction of existing problems

Deploy Audit:

Auto-register new (multiple) versions of components / apps
Prove everything got deployed correctly
Detect wrong versions, missed changes, incomplete backout
REST APIs allow total integration with DevOps tool chain

Demonstration: Error Scan

Video Available on Youtube at: https://youtu.be/CVJNpc0souk

Performance: How Long Does It Take?

Verify Sys1.Linklib (4162 modules)

- Quick scan: **< 0.01 sec CPU,** 1 second elapsed
  About 1 million module scan in 2 CPU seconds
- Full Scan: **< 2 sec CPU, < 1** minute elapsed
  Uses z hardware assist – Crypto / Hashing

Verify APF list (149 Datasets, 42,600 modules)

- Quick scan: **1 sec CPU,** 15 seconds elapsed
- Full Scan: **36 sec CPU,** 4 minutes elapsed

Install 1 hour, results hour 2

Quick scans anytime, Full Scans at night CPU impact – ZERO

All tests conducted at IBM's Dallas Innovation Center on an EC12 w/ ICSF running z/OS 2.2

APF Scan – Self Defining

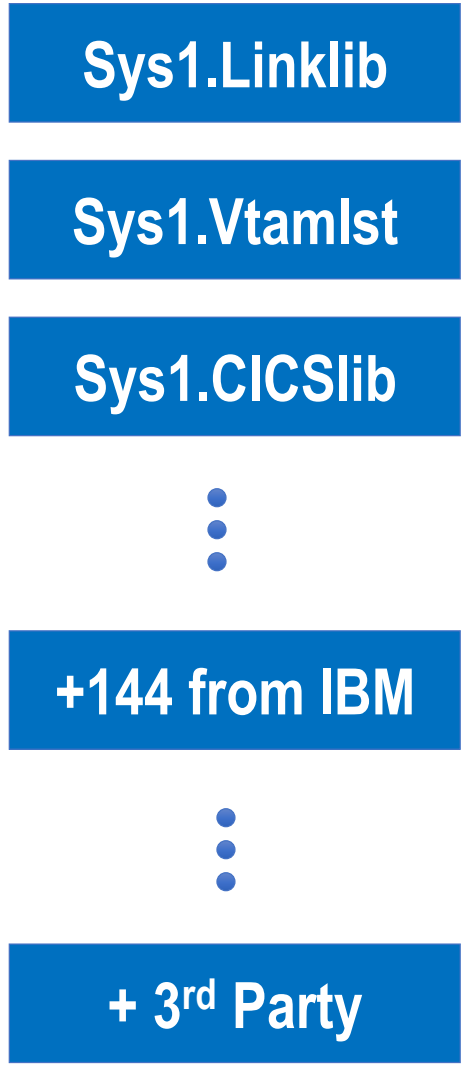
Meant to run automatically – no manual intervention

Scan every APF executable in actually in use

- FIM+ invokes CVSAPF for module list (42,000+)
- Dynamically select all APF libraries – no admin
- Scan executables to create a baseline
- Monitor makes sure modules in use stay correct

As noted – uses less than 1 sec CPU

No set-up, No admin – Just results



Demonstration: Self-Defined APF Scan

Video Available on Youtube at: https://youtu.be/Dx9mfrnqdDc

I've Already Got It Covered

IBM, CA, BMC… don't provide real FIM tools

- RACF, ACF2, TSS – access control, not verification
- Splunk, QRadar and other SIEMs – track events, not correctness
- Endevor, ChangeMan, ISPW – build change packages, not audit

One event monitoring company goes so far as to say*

> *"Effectively, there is no native z/OS program that can facilitate FIM on the mainframe"*

…Guess they missed the memo

*InfoSec Myths Debunked https://cdn2.hubspot.net/hubfs/121847/docs/correlog-maimframe-fim-whitepaper-2016-1-hubspot.pdf

False Alarms?

Every Security Product Has False Alarms – So many they get ignored

- Results in 197 days (or more) to detect a breach
- Need more alarms or real alarms?
- AI won't help flawed event data

Suspicious Alarm? Verify it with FIM+

- FIM+ becomes the source of truth for other tools
- Are components correct? Then it's likely a false positive
- Is it just a wrong level? Then it is likely an accidental update
- Or is it truly suspicious

FIM+ Focusses Incident Response

- Verify problem is real
- Reveals scope – how many systems affected
- Determines attack interval – since the last scan success
- Initiate query of event logs

Save Time? Save Costs?

I Can't Keep Up Now - No Time for Install & Admin

FIM+

- Validates event monitor data eliminating over 90% of false alarms
- Delivers **No Admin** features – like APF scan, Catalog list, etc
- Integrates with other products ServiceNow, Splunk …..
- Imbeds FIM+ in DevOps build / deliver tool chain (validate SCM, Deploy …
- Provides real Audit - takes less time by eliminating redundant data gathering

Save time the first day, and every day

No Budget / Work Plan

- FIM+ pays for itself – reduced outside audit fees

Many Problems, One Solution

Hacking, Errors, Glitches - All involve changes to files

Fortunately:

- File Integrity Monitoring can detect all three using the same method
- Several quick win solutions exist to reduce the likelihood of an issue

Remember:

- Most damage results from breaches over 6 months old
- How does that look? Who gets hung out…is it you?

What can You Do?

1. Do an express trial and see for yourself
2. Give your auditors what they really want so you can get back to work faster

Hoping No One Hacks Your Mainframe is a Poor Defense

So now you know

Proven - FIM+ is the Only z/OS product that can:

- Deliver OnDemand verification that software levels are correct – or not
- Provide absolute proof of compliance with PCI, NIST and other requirements
- Get through your next audit in ½ the time
- Synchronize multiple LPARs and applications
- Verify approved changes are correct before the Monday blues
- Fix known integrity exposures such as SMP/E injection
- Detect internal attacks rigorously
- Eliminate False Positives in other products

Start saving your time and money today

Still Not Convinced?

A one day free trial?

Early support trials:

- 1 hour install - No application or security changes
  Using self-install features like dynamic vault allocate
- Immediate use of APF scan commands, system sync features
- Guided install support from our senior technicians

What you'll get:

- FIM+ - Proves that in use components are correct – or not
- Results - in one hour you'll reveal system secrets you never knew

To request a trial just call us (403) 818-8625 or email info@maintegrity.com

Thank You

Your time is valuable

Thankyou for spending it with

We believe it will turn out to be a great investment

Now how about some questions?

To get hold of us later:

Al Saurette	(403) 818-8625	al@maintegrity.com
Brandon Saurette	(587) 897-7502	brandon@maintegrity.com