MAINTEGRITY

New Ways to Maintain Integrity

FIM+ System Integrity

Partners:

PCI Security Standards Council

IBM Registered Business Partner

splunk>

Presented By:	Gary Euler	(403) 542-3162	Gary@maintegrity.com
	Al Saurette	(403) 818-8625	Al@maintegrity.com

Agenda

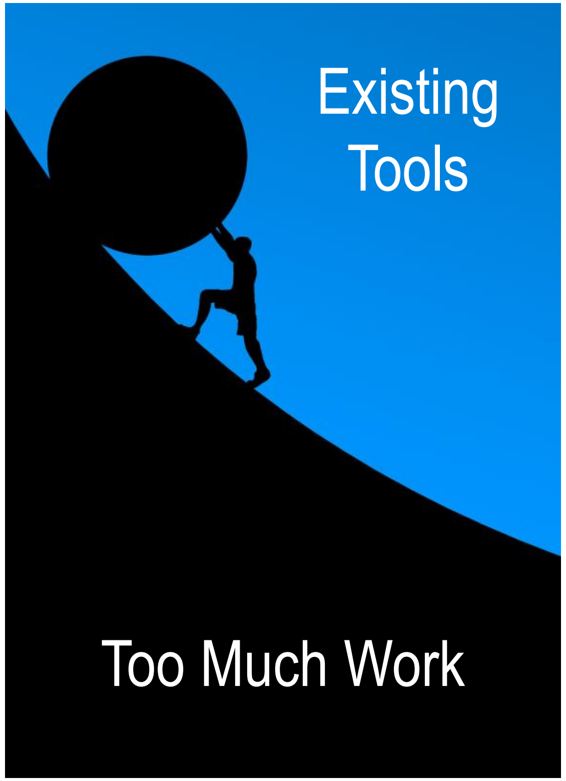
- MainTegrity Background
- FIM+ Need
- FIM+ Overview
- FIM+ Security and Compliance
- FIM+ Integrity Management
- FIM+ Usability and GUI Walkthrough
- Wrap-up and questions

Background

- Principals involved in Enterprise Software since the late 1980's
  - Products include Harbor, Stand Alone Environment, ISPW
- 2014, FIM+ concept started as a verification tool for application rollouts
- 2017, notice FIM technology would be PCI/DSS requirement in Jan 2018
- No mainframe FIM solution existed
  - Form a company (MainTegrity),
  - Develop a FIM product for operational folks - highly automated, feature rich
- Initially detection only – now gather forensics / assist with recovery
- Financing completed in August of 2018

Imagine a mainframe software start up in 2017… who would of thought

Customer Challenges



Do you need to?

- Improve internal security and compliance (PCI/DSS, GDPR, NIST)
- Manage system integrity across multiple clients, systems or LPARs
- Audit / Certify software is correct (on demand or continuous)
- Monitor system and configuration file changes (compare in stream)
- Give a new generation of support staff the tools to do things right
    - Present info from differing tools (SMF, ServiceNow, Remedy, Splunk, QRadar, etc)

Business Need

MAINTEGRITY

2019 IBM / Ponemon report

- +500 organizations surveyed
- Detection – **206 days**
- Respond & Recover – **+73 days**

Why you should care

- Average breach cost: $4.3 Million
- Brand / reputation impact
- You may lose your job

Root Cause

Malicious Attack - 51%	Outsider breaking in
Human Errors - 25%	Insiders making errors
System Glitches - 24%	Corrupt files, bad configs

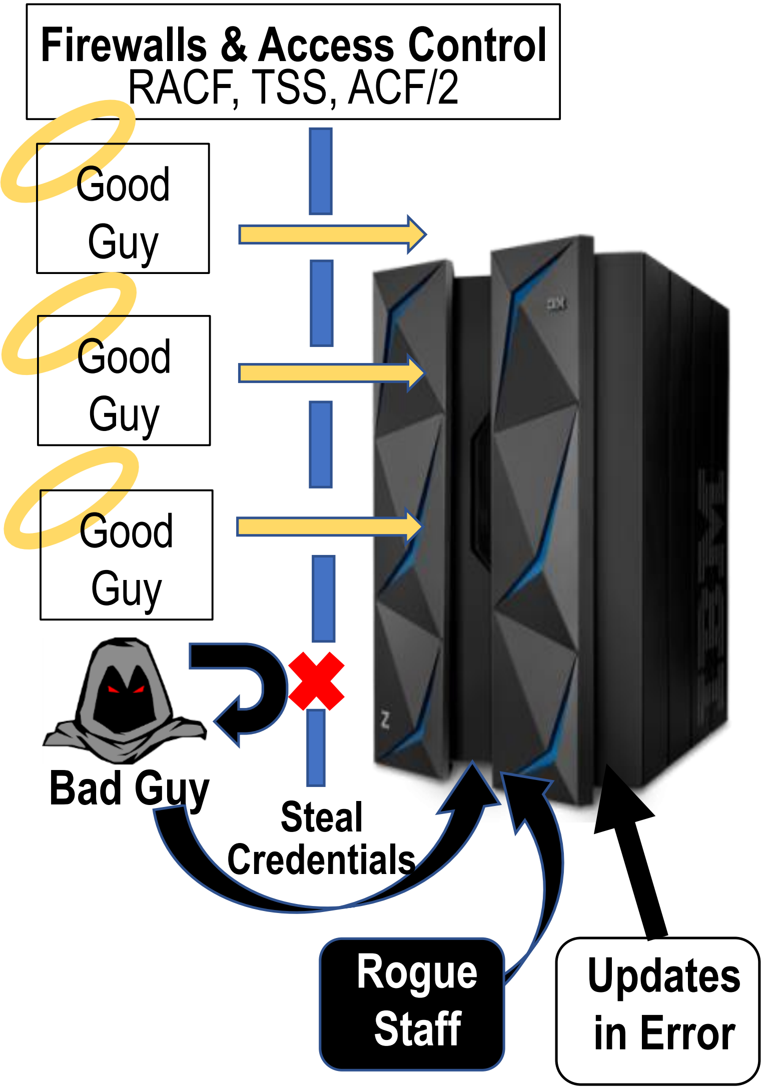
Errors not resulting in data breaches not reported

Mainframes matter

- $7.7 trillion credit card payments (annual)
- 29 billion ATM transactions (annual)
- 87% of credit card transactions

IBM sponsored 2019 Ponemon *Cost of Data Breach Study*

Need - Why Bother?



Conventional Security – Guard the perimeter

- Insiders are past Firewall / Access Control
    1. Steal Credentials (phishing, man-in-middle, guessing, etc)
    2. Trusted employees go rogue (addiction, financial, health)

Well meaning staff make mistakes (deploy, update)

- Were the changes correct?
- Are all the LPARS the same? Exceptions?
- Traditional monitoring is manual (Labor intensive)
- Requires lots of z/OS specific skills

Overview - What Does FIM+ Do?

File Integrity Monitoring (FIM)

- Creates a hash key for each files at a trusted level
- Save key in an encrypted vault
- Later create another hash key and compare the keys.

Monitor major mainframe files automatically

- z/OS system, CICS, IMS, DB2, TCP/IP, application executables, JCL, configs …
- USS files, Scripts, Clists, Log files, encrypted data sets

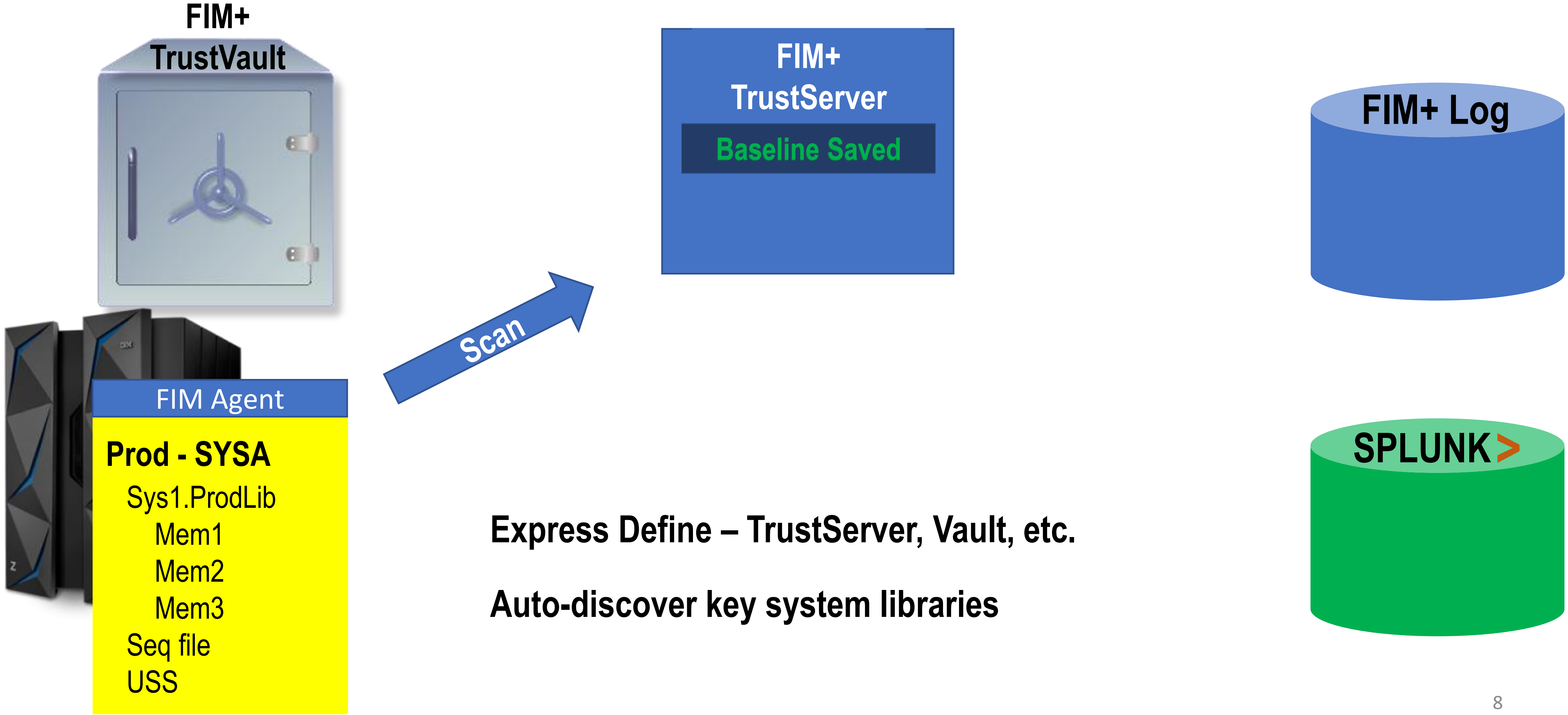
Alerts

- Alerts sent via Text or Email to admin or central console
- 4 click drill down to forensic info (SMF, change control, etc)

High Performance

- Offload to crypto card, minimal CPU

Overview - Getting Started with FIM+



FIM+ TrustVault

FIM Agent

Prod - SYSA

- Sys1.ProdLib
  - Mem1
  - Mem2
  - Mem3
- Seq file
- USS

FIM+ TrustServer

Baseline Saved

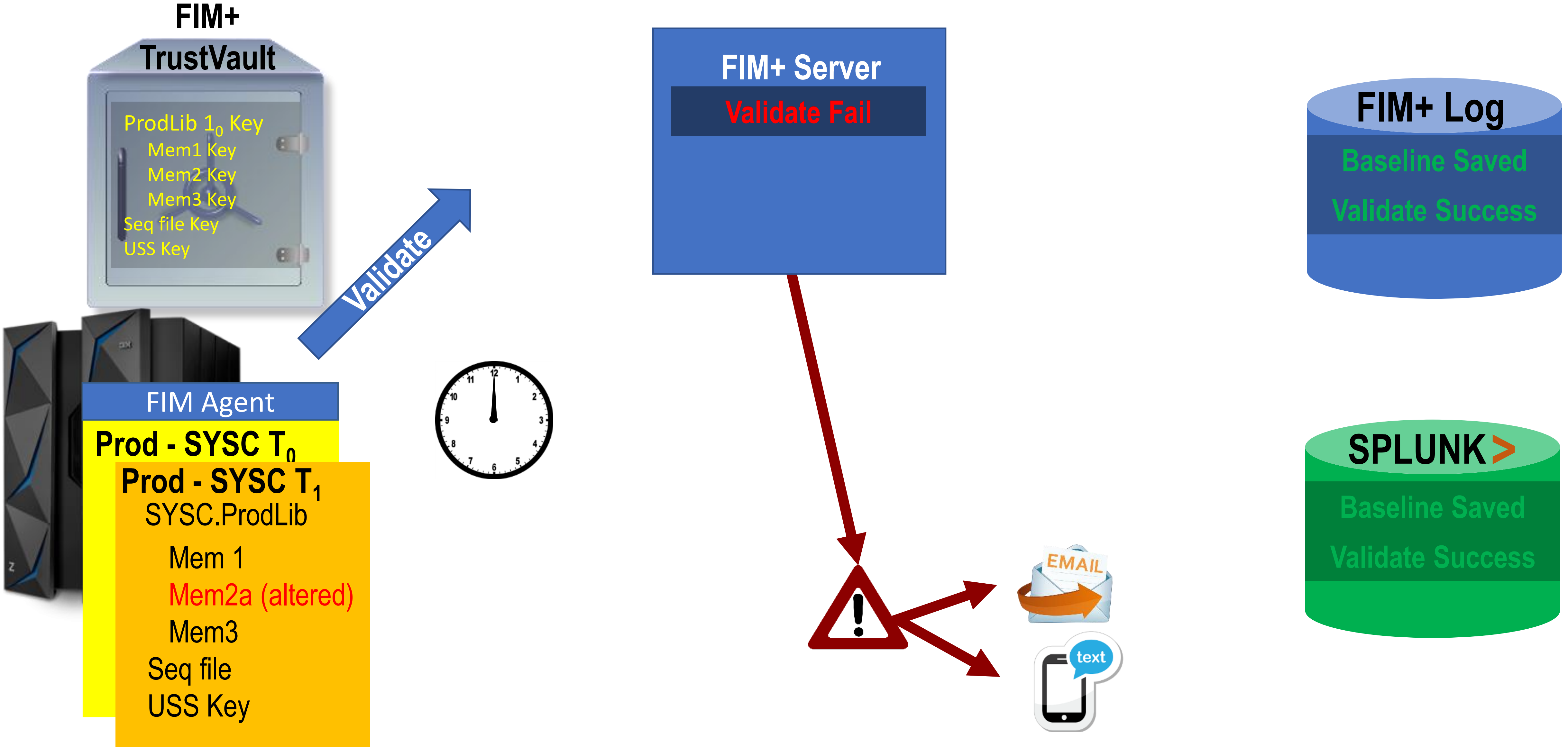
FIM+ Log

SPLUNK>

Express Define – TrustServer, Vault, etc.

Auto-discover key system libraries

Overview - Change Detected



FIM+
TrustVault

ProdLib 1_0 Key
Mem1 Key
Mem2 Key
Mem3 Key
Seq file Key
USS Key

Validate

FIM Agent

Prod - SYSC T_0

Prod - SYSC T_1
SYSC.ProdLib
Mem 1
Mem2a (altered)
Mem3
Seq file
USS Key

FIM+ Server
Validate Fail

FIM+ Log
Baseline Saved
Validate Success

SPLUNK>
Baseline Saved
Validate Success

Better change detection

Bit by bit clarity that code / configs are still correct

- Validates file contents by scanning the actual file
- Zero false alarm initiative
  - Corroborate alarms are real
  - Suppress approved changes
  - Interoperate with change management systems
- Audit application and system deployments
  - Ensure code levels in all LPARS are the same
  - Detect wrong versions, missed changes, and backout errors
  - Before and After FIM+ snapshots prove everything got deployed correctly

Integrity Management

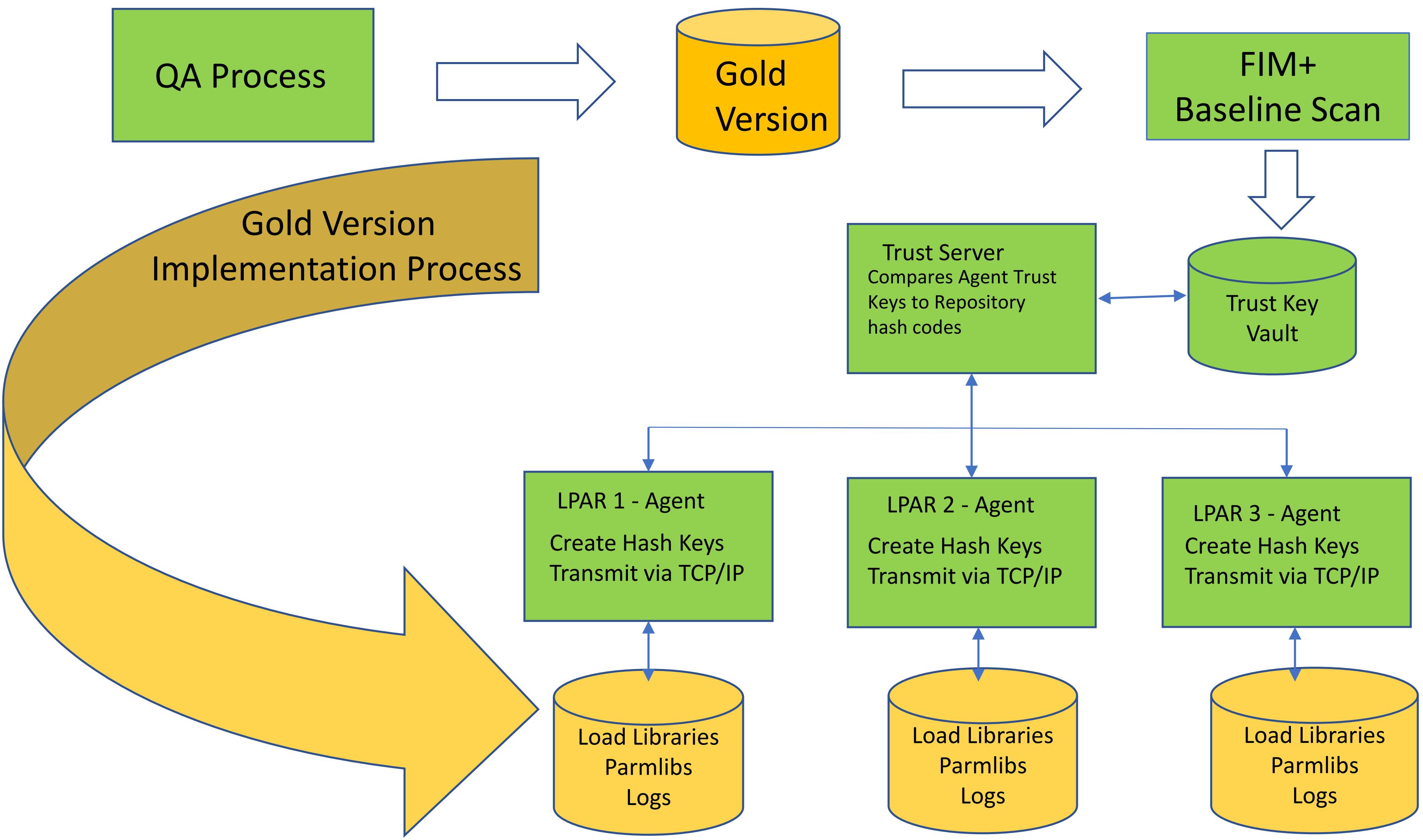
Problem:

- Systems and apps on multiple LPARS need to be rolled out correctly
- Accommodate required LPAR specific deviations
- People with legitimate credentials make unauthorized or inadvertent changes
  - Code tends to drift from the base over time
- If a problem occurs in only one LPAR, determining what is / should be different is daunting.
- Ongoing audits to prove production systems are correct are manual – hence not done.

Solution – FIM+:

- Define a version of the application as the baseline and compare the code base in each LPAR to that baseline version.
- Identify any deviations from the baseline version.
- Continuous Audit is a consequence of implementing FIM+.
- Systems are protected from both inadvertent and malicious changes made using legitimate credentials.
- Advanced forensics are automatically generated to show you who, why, what changes were made.

Integrity Management



Trust vault is encrypted using ICSF

Participating LPARS:

- **need a TCP/IP Connection to the FIM+ Trust Server**
- **Same or different CEC (CPU)**

Integrity Management

System Integrity Management features:

- Baseline Scan
  - Establishes trusted “gold version” as a baseline release
- When a changed file is detected:
  - Detection is logged
  - The proper authorities are notified
  - Complete forensics and compare functions are available through an easy to use GUI
    - Know what changed, who changed it, when & why it changed
    - Compare to baseline version to show actual lines that changed (text based files)
- LPAR specific files
  - Enables the exclusion from comparison to baseline version
- Supports all log file types – GDG’s, Date/Time Stamps, version numbers

FIM+ Usability features

- FIM+ has the following interfaces:
  - GUI, ISPF, Rest API, Batch
- Auto-discovery function monitors:
  - APF Libraries, libraries contained in Started Tasks, libraries added to the system via operator command.
- FIM+ runs 24X7 – supports updates while FIM+ is running
- Integrates with your operational ecosystem
- Initiate scans at predetermined times or on demand
- Complete forensic info gathering and presentation

Human Interface -GUI

FIM+ send text or email alert

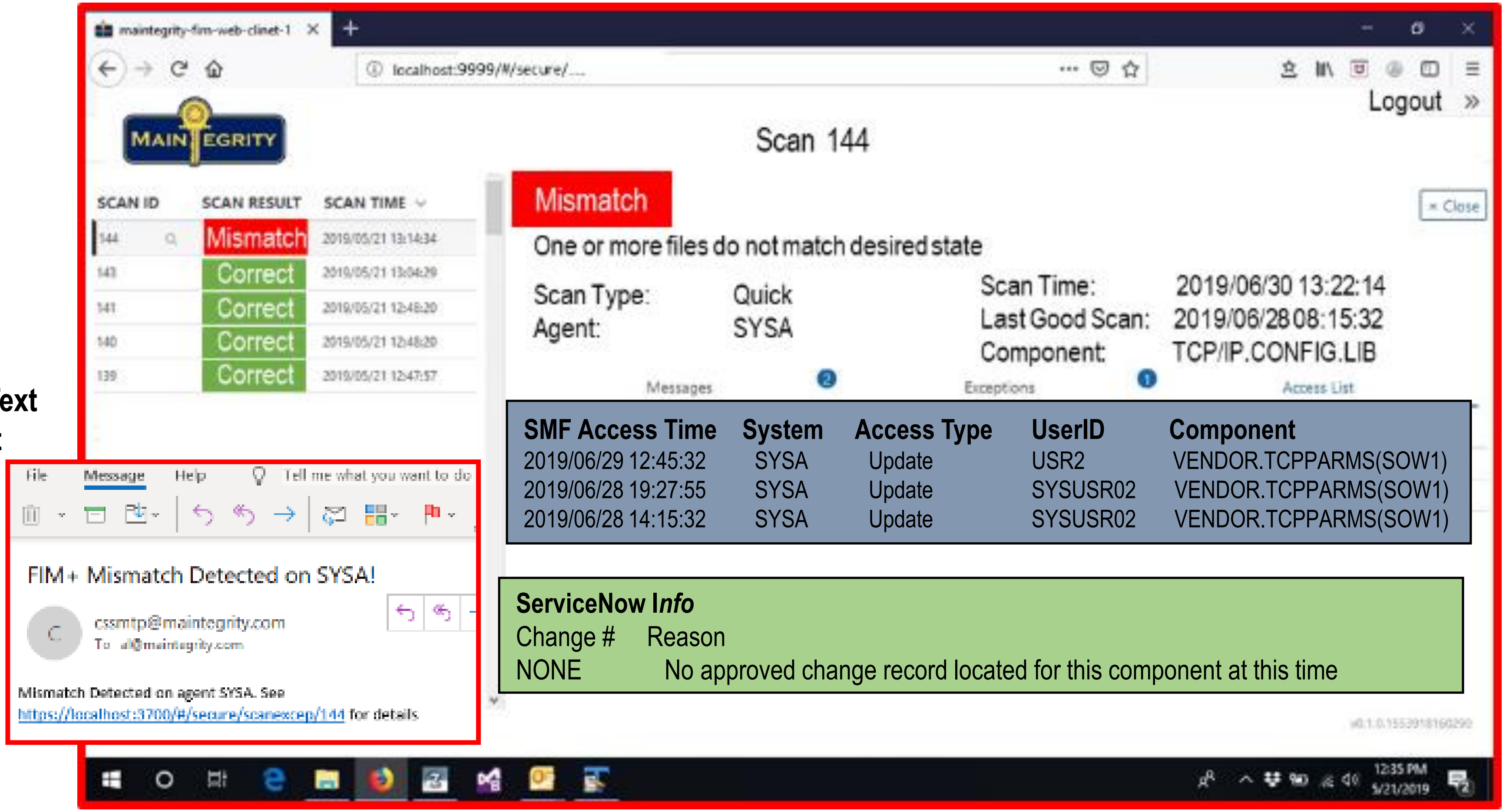
Click 1

When an alert is received one click opens the GUI in any browser and displays detailed info including SMF access data

Click 2

Another click fetches change control info from ServiceNow or Remedy dynamically, without needing mainframe skills.

Email,Text Alert



maintegrity-fim-web-clinet-1
localhost:9999/#/secure/...
Logout
MAINTEGRITY
× Close
Messages
Exceptions
Access List
File
Message
Help
Tell me what you want to do

SCAN ID	SCAN RESULT	SCAN TIME
144	Mismatch	2019/05/21 13:14:34
143	Correct	2019/05/21 13:04:29
141	Correct	2019/05/21 12:48:20
140	Correct	2019/05/21 12:48:20
139	Correct	2019/05/21 12:47:57

Scan 144

Mismatch

One or more files do not match desired state

Scan Type: Quick
Agent: SYSA

Scan Time: 2019/06/30 13:22:14
Last Good Scan: 2019/06/28 08:15:32
Component: TCP/IP.CONFIG.LIB

SMF Access Time	System	Access Type	UserID	Component
2019/06/29 12:45:32	SYSA	Update	USR2	VENDOR.TCPPARMS(SOW1)
2019/06/28 19:27:55	SYSA	Update	SYSUSR02	VENDOR.TCPPARMS(SOW1)
2019/06/28 14:15:32	SYSA	Update	SYSUSR02	VENDOR.TCPPARMS(SOW1)

ServiceNow *Info*

Change #	Reason
NONE	No approved change record located for this component at this time

FIM+ Mismatch Detected on SYSA!

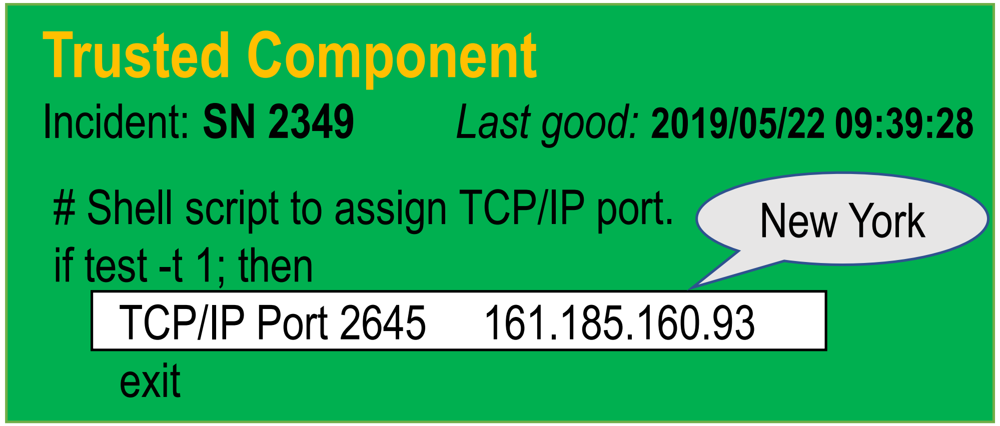
cssmtp@maintegrity.com
To all@maintegrity.com

Mismatch Detected on agent SYSA. See https://localhost:3700/#/secure/scanexcep/144 for details

Human Interface -GUI

Click 3

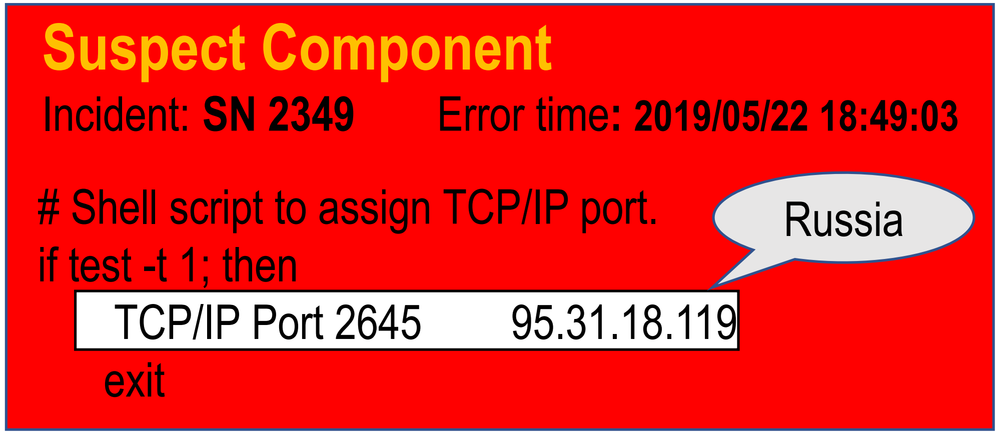
Click 3 can invoke instream file compare to show exactly what line changed.



Trusted Component

Incident: **SN 2349** *Last good:* **2019/05/22 09:39:28**

```
# Shell script to assign TCP/IP port.
if test -t 1; then
  TCP/IP Port 2645     161.185.160.93
  exit
```



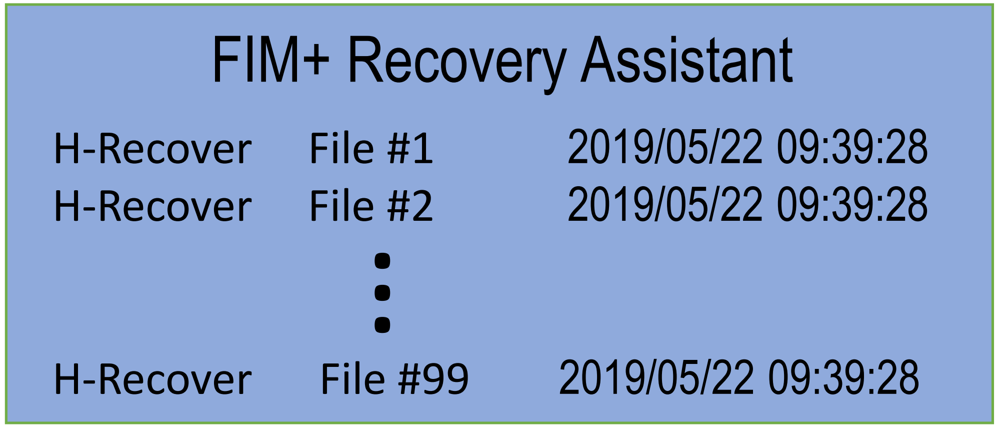
Suspect Component

Incident: **SN 2349** Error time**: 2019/05/22 18:49:03**

```
# Shell script to assign TCP/IP port.
if test -t 1; then
  TCP/IP Port 2645        95.31.18.119
  exit
```

Click 4

Complete restore can be accomplished by clicking the FIM+ Recovery Assistant to select and verify all files required

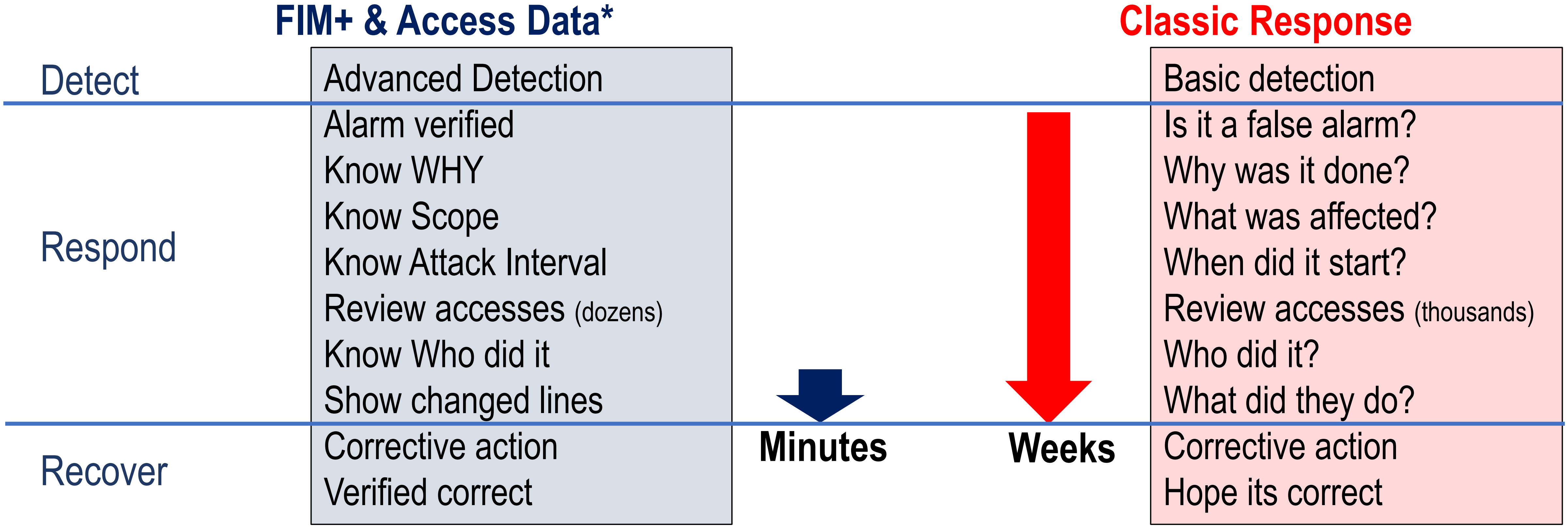


FIM+ Recovery Assistant

```
H-Recover    File #1      2019/05/22 09:39:28
H-Recover    File #2      2019/05/22 09:39:28
                 :
H-Recover    File #99     2019/05/22 09:39:28
```

Power of Automation

Provides quick answers instead of questions, when time is critical



	FIM+ & Access Data*	Classic Response
Detect	Advanced Detection	Basic detection
Respond	Alarm verified Know WHY Know Scope Know Attack Interval Review accesses (dozens) Know Who did it Show changed lines	Is it a false alarm? Why was it done? What was affected? When did it start? Review accesses (thousands) Who did it? What did they do?
Recover	Corrective action Verified correct	Corrective action Hope its correct

Minutes **Weeks**

* Automate forensics / recovery with change info, SMF and FIM+ data at your fingertips

Only FIM+ can:

- Discover APF, subsystem and application components
- Verify software / configs are correct (from SMP/E Dlibs to applications)
- Respond to incidents faster – automated detection / forensics
- Compliance with specific PCI, NIST, GDPR requirements
- Prove content has not changed - real content validation
- Present all relevant info in a GUI (who, what, when, where, why)
- Work with existing tools (SMF, ServiceNow, Remedy, Splunk, QRadar, etc)

Existing tools HOPE changes are correct. FIM+ proves it.

Questions and Wrap-up

Start preventing problems today

- Eliminate false alarms, Automated forensics for the real ones
- Delivers **Zero-Admin** features – like APF scan, Config Scan, Appl versioning, etc
- Give deploy team real validation - within the change window

Save time the first day, and every day

- If a problem occurs - Who gets hung out? Make sure its not you

Find out more:

- Book a deep dive demo or a free trial – with no obligation - today

Mainframes are high value targets – Defend them properly