MAINTEGRITY

a

# June 8 Presentation

**Partners:**

bmc

IBM Registered Business Partner

PCI Security Standards Council

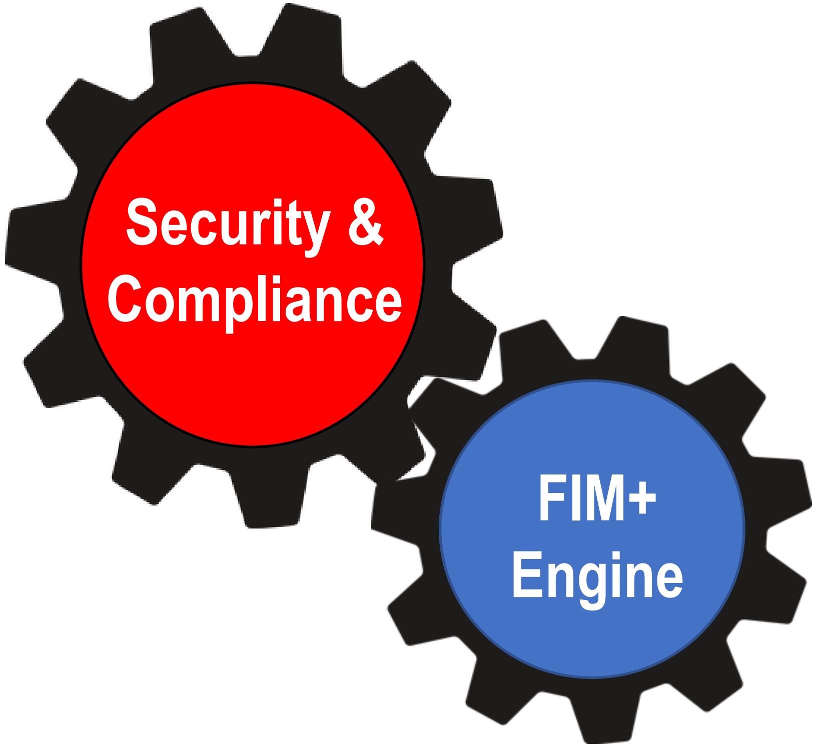
splunk>

Al Saurette (Al@Maintegrity.com) MainTegrity

Gary Euler (Gary@MainTegrity.com) MainTegrity

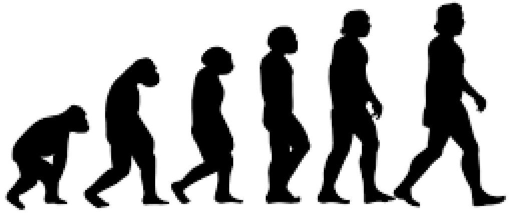
# What you will learn

- Why FIM+ can improve:
  - Your  z/OS Security,
  - Response to Security incidents
  - Save time and Improve PCI compliance
- Hacker Evolution – Very Scary
- Why perimeter security is not enough
- Inside a Ransomware attack
- Anatomy of the ATM Cash-out attack
- PCI recommendations
- Questions and Wrap Up



# The rise of hackers

| Type of Attack | Date started | Goal of attack | Who commits the attack |
|---|---|---|---|
| Penetration | 70's and 80's | Impress other hackers | Lone wolf |
| Viruses | 1987(Brain)<br>1994(AOHell)<br>2000(ILOVEYOU) | Annoy people, Activism, Free Internet, Steal Credit Cards | Lone wolf or small teams |
| Denial of Service | 1996 (Panix) | Revenge, Money, activism | Lone wolf or small teams |
| Ransomware | 1989(Aids Trojan) | $$ | Lone wolf >>> to sophisticated teams |
| Ransomware as a service | 2005ish | $$$ | Small sophisticated teams, organized crime |
| Cyber warfare | 2010ish (Stuxnet) | $$$$, Secrets, disrupt life, shut down infrastructure, mayhem | Big, well funded Nation State Attacks |



Looking for much bigger game

# The Threat

## Mainframes stats (ATMs and IMS)

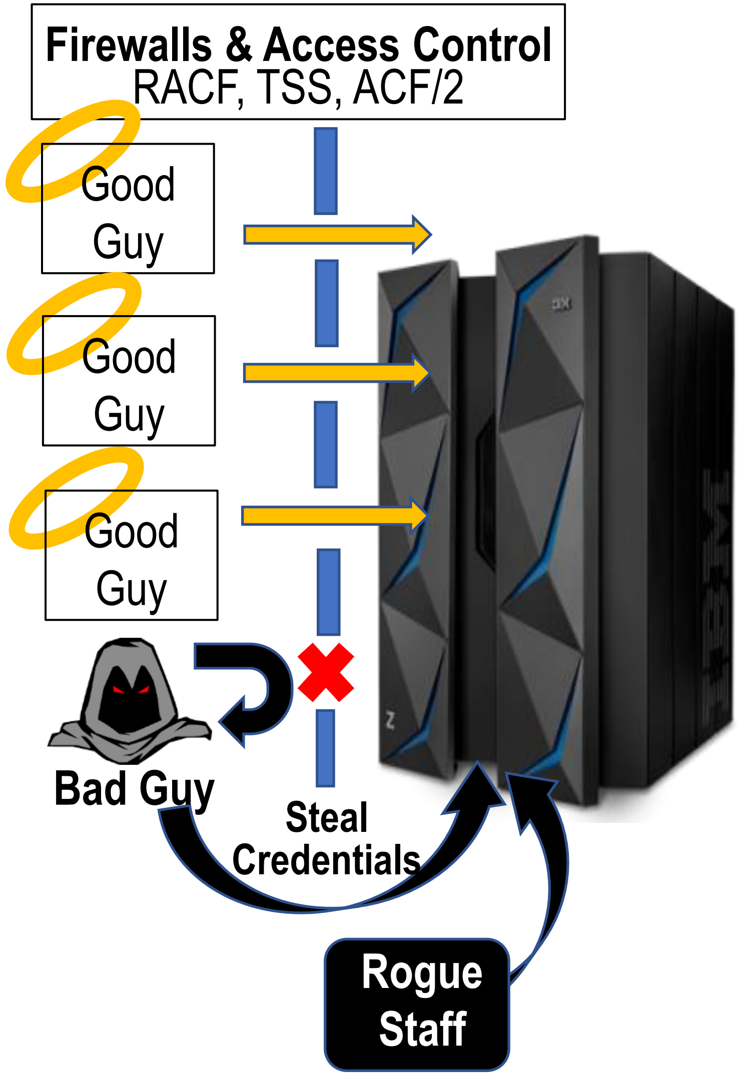
- $7.7 trillion credit card payments (annual)
- 29 billion ATM transactions (annual)
- 12.6 billion transactions (daily)
- 87% of CC Transactions done on z/OS

## The IT world is increasingly unsafe

- Dark web many millions of userid / PW for sale – Troy Hunt [1]
- Organized Crime and Nation States increasingly involved
- Increasingly, Governments are calling for 'zero trust' cyber infrastructures

[1] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach

# Conventional z/OS security



## Guard the perimeter

- Insiders are past Firewall / Access Control
  1. Bad Guys steal credentials (look legitimate)
  2. Trusted employees go rogue (disgruntled, gambling, health)

No matter how good your perimeter defences are criminals can get in

Forrester says ‘Perimeter security has FAILED”

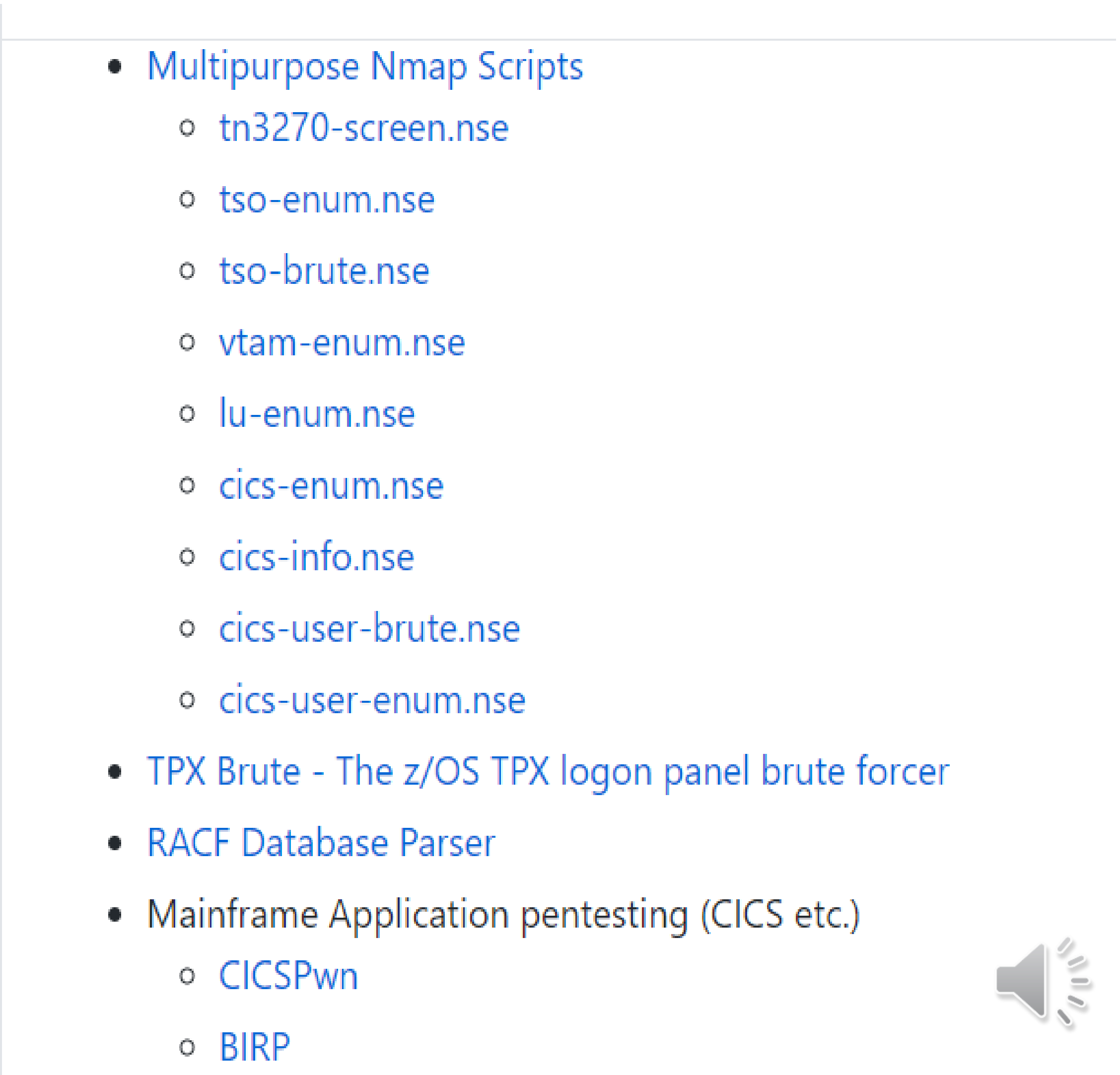
# Mainframe Hacking Tools

A simple Google search turns up an impressive array of z/OS Hacking tools:

My favourite are the **Z/OS System Enumeration Scripts:**

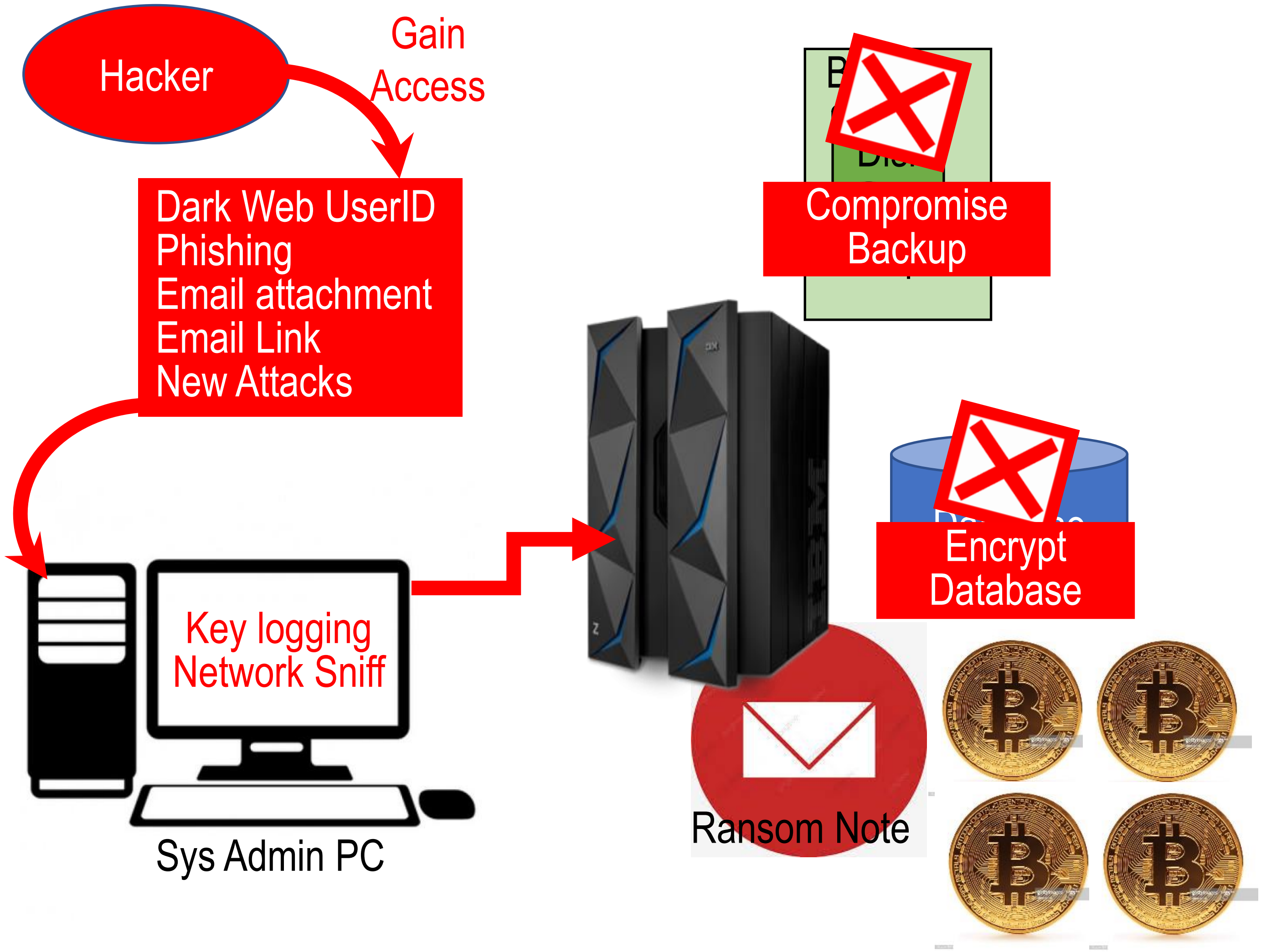
```
ENUM - Display APF Datasets, Catalogs, RACF Information, all
SVC’s,

STARTMAP – Display IPL Information, Proclibs

CATMAP – Walks a catalog and gathers PDS and PDSE member names

SYSOWN- List of libraries and their meta data of the files in
this TSO Session.
```

One wonders what is available on the Dark Web (Tor)



- Multipurpose Nmap Scripts
  - tn3270-screen.nse
  - tso-enum.nse
  - tso-brute.nse
  - vtam-enum.nse
  - lu-enum.nse
  - cics-enum.nse
  - cics-info.nse
  - cics-user-brute.nse
  - cics-user-enum.nse
- TPX Brute - The z/OS TPX logon panel brute forcer
- RACF Database Parser
- Mainframe Application pentesting (CICS etc.)
  - CICSPwn
  - BIRP

# Anatomy of a z/OS Ransomware Attack



Hacker

Gain Access

Dark Web UserID
Phishing
Email attachment
Email Link
New Attacks

Key logging
Network Sniff

Sys Admin PC

Compromise Backup

Encrypt Database

Ransom Note

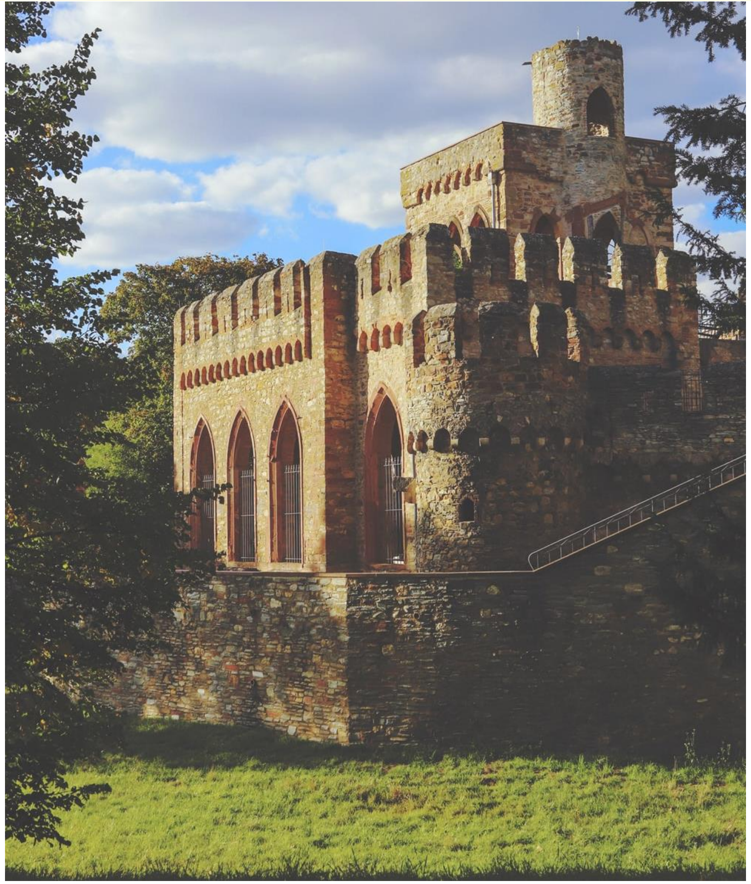
## Steps in an Advanced Ransomware Attack[1]

- Reconnaissance
- Penetrate
- Fortify
- Infiltrate
- Spoliation
- Ransom Demand

[1] Eric Vanderburg: The Six Phases of an Advanced RansomWare Threat
https://www.tcdi.com/6-phases-advanced-ransomware-threat/

# FIM+ Ransomware Solutions

- Whitelisting[1] – FIM+ discovers/monitors key elements
- Integrity verify on backups[2] - Checksum
- Real-time access and FIM alerts via email / text
- Forensic data gathering / display – SMF, approvals
- Policy driven actions:
  - File quarantine, deletion
  - Guilty Userid suspension
- Audit records to prove compliance – PCI, NIST, GDPR



Creating a z/OS data fortress

[1] NIST – Guide to Application Whitelisting – October 2015

[2] European Central Bank,  Cyber resilience oversight, Dec 2018

# Application & System Whitelisting

“Use application whitelisting, which only allows systems to execute programs known and permitted by security policy. ” [1]

“A *whitelist* is a list of discrete entities, …. processes, or applications that are authorized to be present or active on a system according to a well- defined baseline. ” **[2]**

**White listing with FIM+:**

- Auto Discover for APF and Program Product Libraries (IMS, CICS, DB2 etc) to create baselines
- Application scan – create a baseline from any selected applications immediately after QA
- Active enforcement – FIM+ monitors the whitelist and sends an alert if any change is detected
- Support for Multiple Versions – Baselines can created on demand

**Benefit:**

- Malware cannot get placed on your production system without triggering an alert
- Security team notifications and responses occur automatically

[1] How to protect your networks from Ransomware– US Government Inter Agency Document
https://www.justice.gov/criminal-ccips/file/872771/download
[2] NIST – Guide to Application Whitelisting – October 2015
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

# Checksums on Backups

**Central Banks in North American and Europe recommend commercial banks perform checksums on backups. ECB says “Backups should be tested regularly to verify their availability and integrity.” [1]**

## WHY?:

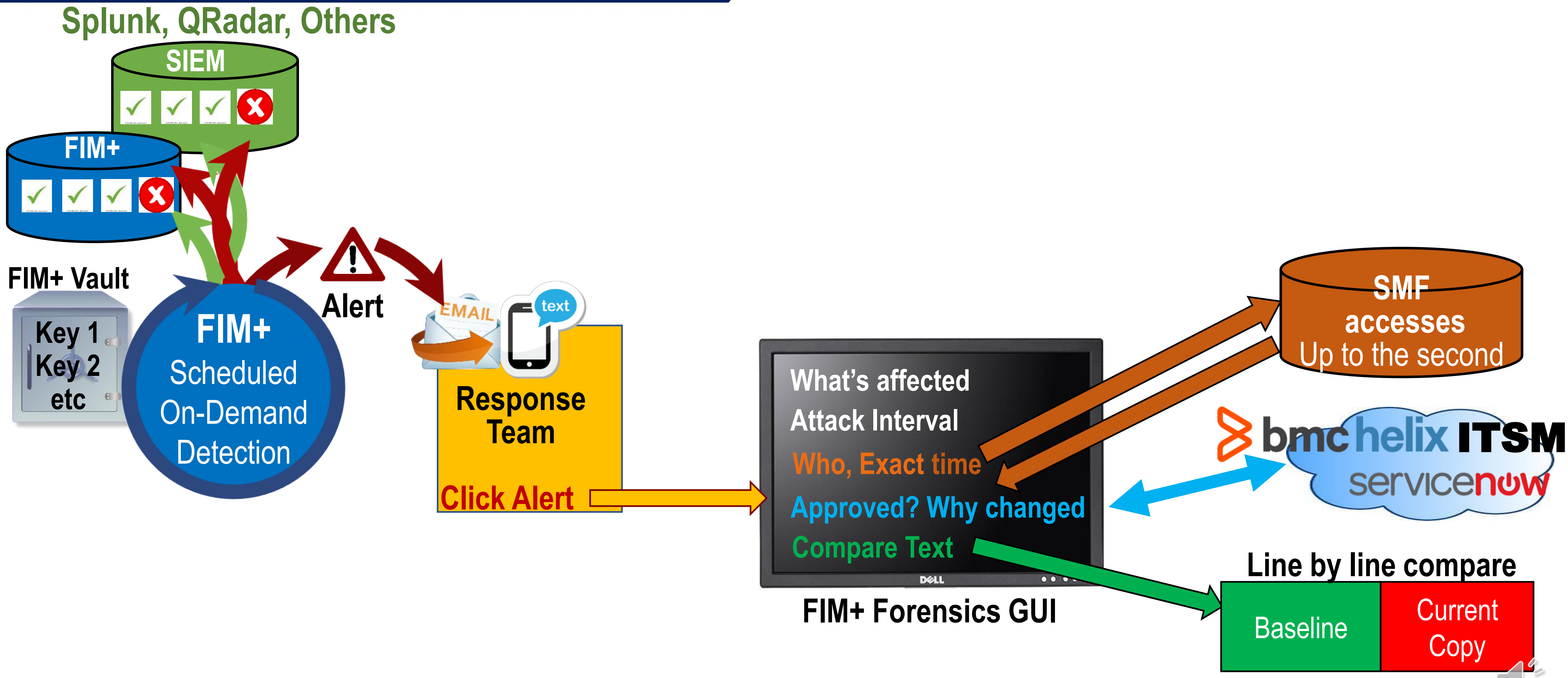
- Provide early warning of an impending Ransomware attack.
- A ransomware attack could impact the Financial Market stability

## SOLUTION:

- Full scans for smaller backup files
- Sample Scans for handling terabyte sized backup files
  - Creates key from a user definable amount of data in the file
  - Can do sample scans with periodic full scans or just sample scans
  - Can sample the same data or different data on each scan
  - Can read first and last block only (Virtual Tape)

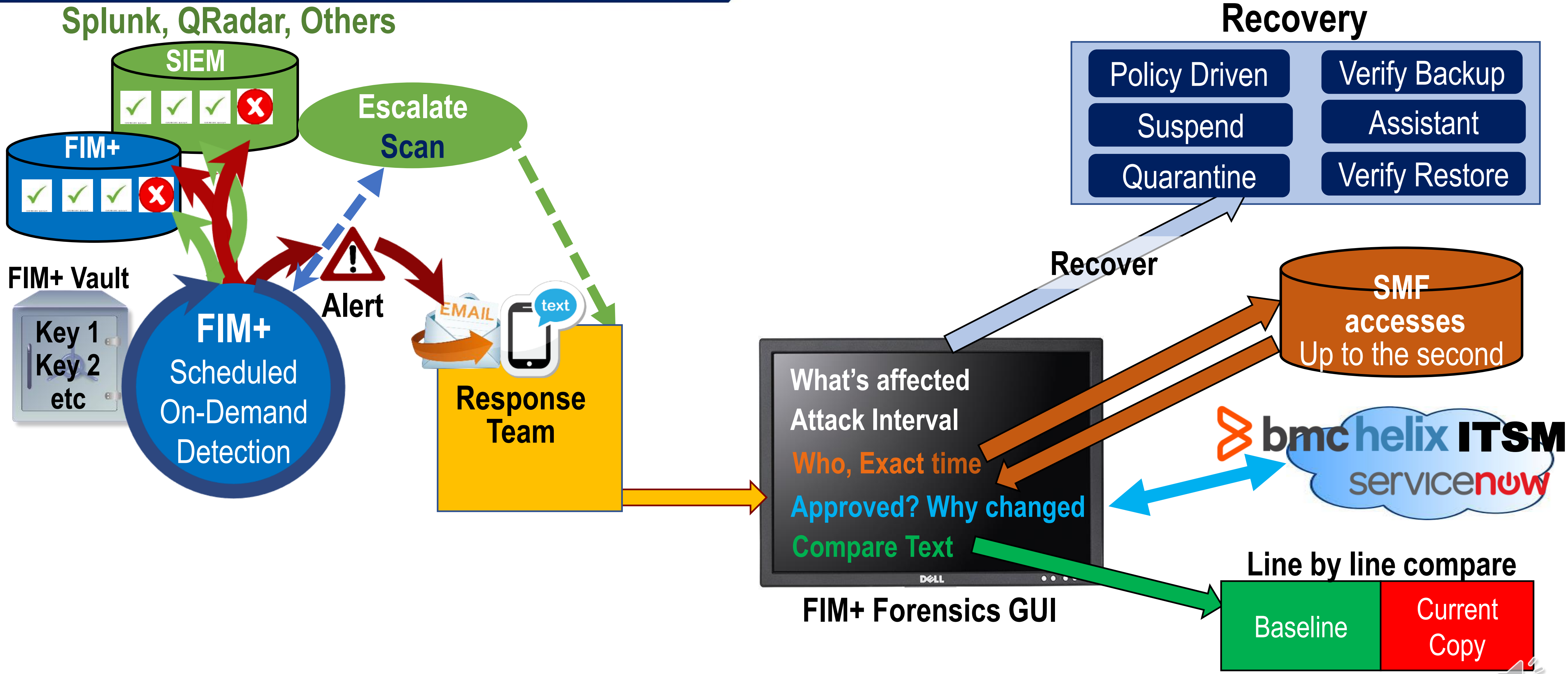
[1] European Central Bank, Cyber Resilience Oversight, Dec 2018
https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

# FIM+ Detection



Manage, Detect, Respond, Recover

# FIM+ Recovery



Splunk, QRadar, Others

SIEM

FIM+

FIM+ Vault

Key 1
Key 2
etc

FIM+
Scheduled
On-Demand
Detection

Escalate
Scan

Alert

EMAIL

text

Response
Team

FIM+ Forensics GUI

What's affected

Attack Interval

Who, Exact time

Approved? Why changed

Compare Text

Recover

Recovery

| | |
|---|---|
| Policy Driven | Verify Backup |
| Suspend | Assistant |
| Quarantine | Verify Restore |

SMF
accesses
Up to the second

bmc helix ITSM

servicenow

Line by line compare

| Baseline | Current Copy |
|---|---|

Manage, Detect, Respond, Recover

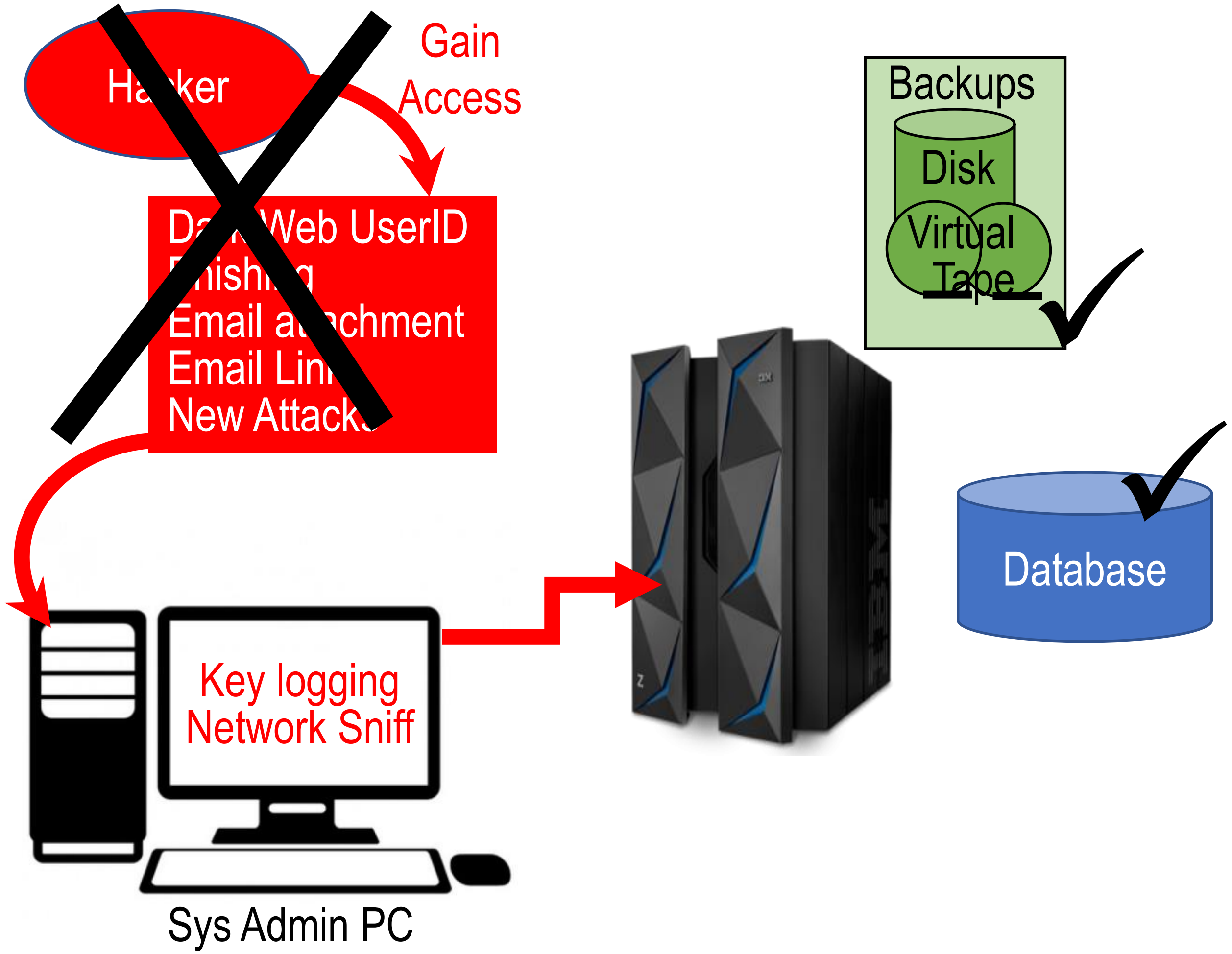
# The Bottom Line

Provide quick answers instead of questions, when time is crucial

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

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

# Now defeat Ransomware



Hacker

Gain Access

Dark Web UserID
Phishing
Email attachment
Email Link
New Attacks

Key logging
Network Sniff

Sys Admin PC

Backups
Disk
Virtual Tape

Database

## What has FIM+ done for you?

- Verified Backups
- Sent Early Warning
- Real-time Alerts
- Fast reaction – Forensics
- Scope - what else was affected
- Prevented a ransom attack

Defeat Ransomware & other Malicious exposures – Now!

# PCI and FIM

## Payment Card Industry Data Security Standard

| | |
|---|---|
| Sec 10.5.5 | Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)? |
| Sec 11.5 | Is a change-detection mechanism (for example, **file-integrity monitoring tools**) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files? |

PCi Security Standards Council ®

**Section 3: …..Part 3. PCI DSS Validation**

☑ **Compliant:** All sections of PCI DSS complete, all questions answered affirmatively

**Part 3b. Attestation** C

*Signature of Executive Officer* ___________________________________

*Executive Officer Name:* ______________________________ *Date:*

*Title: _Your CIO, Your CFO, Your CEO_*

Without FIM technology you do not comply. Period

# Recent ATM Hack

Key Points in attack:

- Most ATM transactions captured by IMS on a mainframe
- Card management system is altered
- Change to parameters or executable
- Takes knowledge / coordination - most likely ‘inside job”

Recommended best practices?

1. 24/7 monitoring with File Integrity Monitoring (FIM)
2. Improve detection, response, recovery
3. Strict separation of roles - no “inside job”

**October 7, 2020**

**BULLETIN: ATM CASH-OUT THREAT**

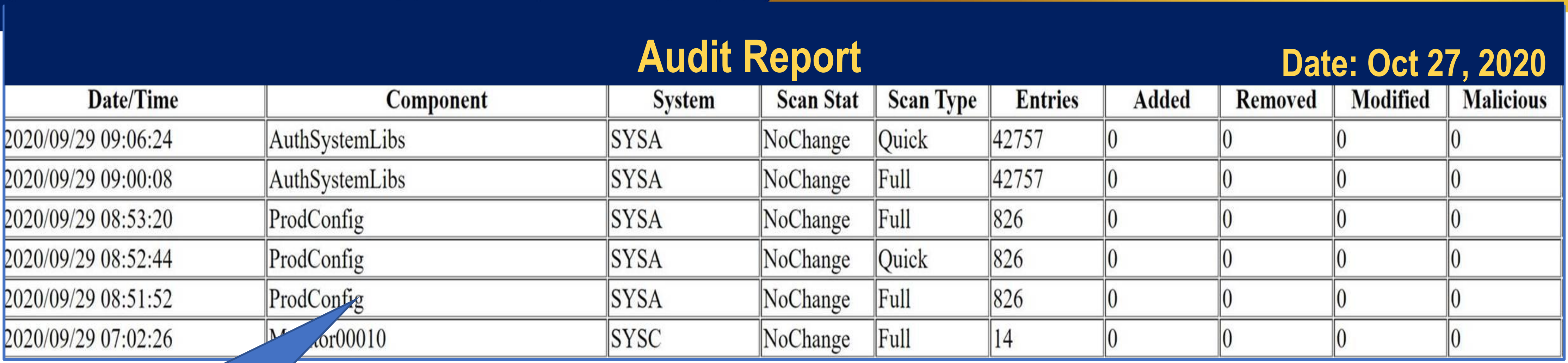
The PCI Security Standards Council and ATM Industry Association want to highlight an emerging threat that requires **urgent attention.**

**What is the threat?**

ATM “cash-out” attack is an elaborate attack in which criminals breach a bank or card processor and manipulate fraud detection controls as well as customer accounts

Also stronger NIST, GDPR, Bank Resiliency ….

# Proof of Compliance



## Audit Report

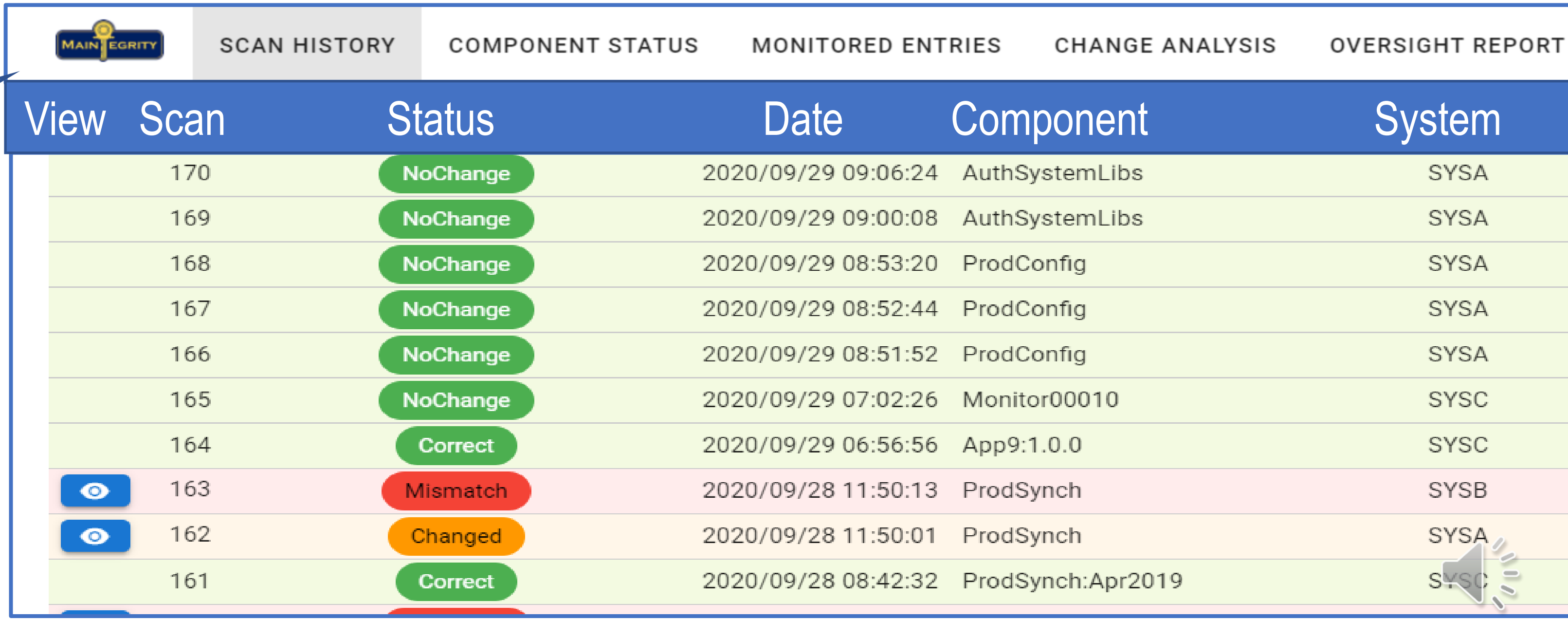
Date: Oct 27, 2020

| Date/Time | Component | System | Scan Stat | Scan Type | Entries | Added | Removed | Modified | Malicious |
|---|---|---|---|---|---|---|---|---|---|
| 2020/09/29 09:06:24 | AuthSystemLibs | SYSA | NoChange | Quick | 42757 | 0 | 0 | 0 | 0 |
| 2020/09/29 09:00:08 | AuthSystemLibs | SYSA | NoChange | Full | 42757 | 0 | 0 | 0 | 0 |
| 2020/09/29 08:53:20 | ProdConfig | SYSA | NoChange | Full | 826 | 0 | 0 | 0 | 0 |
| 2020/09/29 08:52:44 | ProdConfig | SYSA | NoChange | Quick | 826 | 0 | 0 | 0 | 0 |
| 2020/09/29 08:51:52 | ProdConfig | SYSA | NoChange | Full | 826 | 0 | 0 | 0 | 0 |
| 2020/09/29 07:02:26 | Monitor00010 | SYSC | NoChange | Full | 14 | 0 | 0 | 0 | 0 |

Compliance Report

On-Demand Browser View

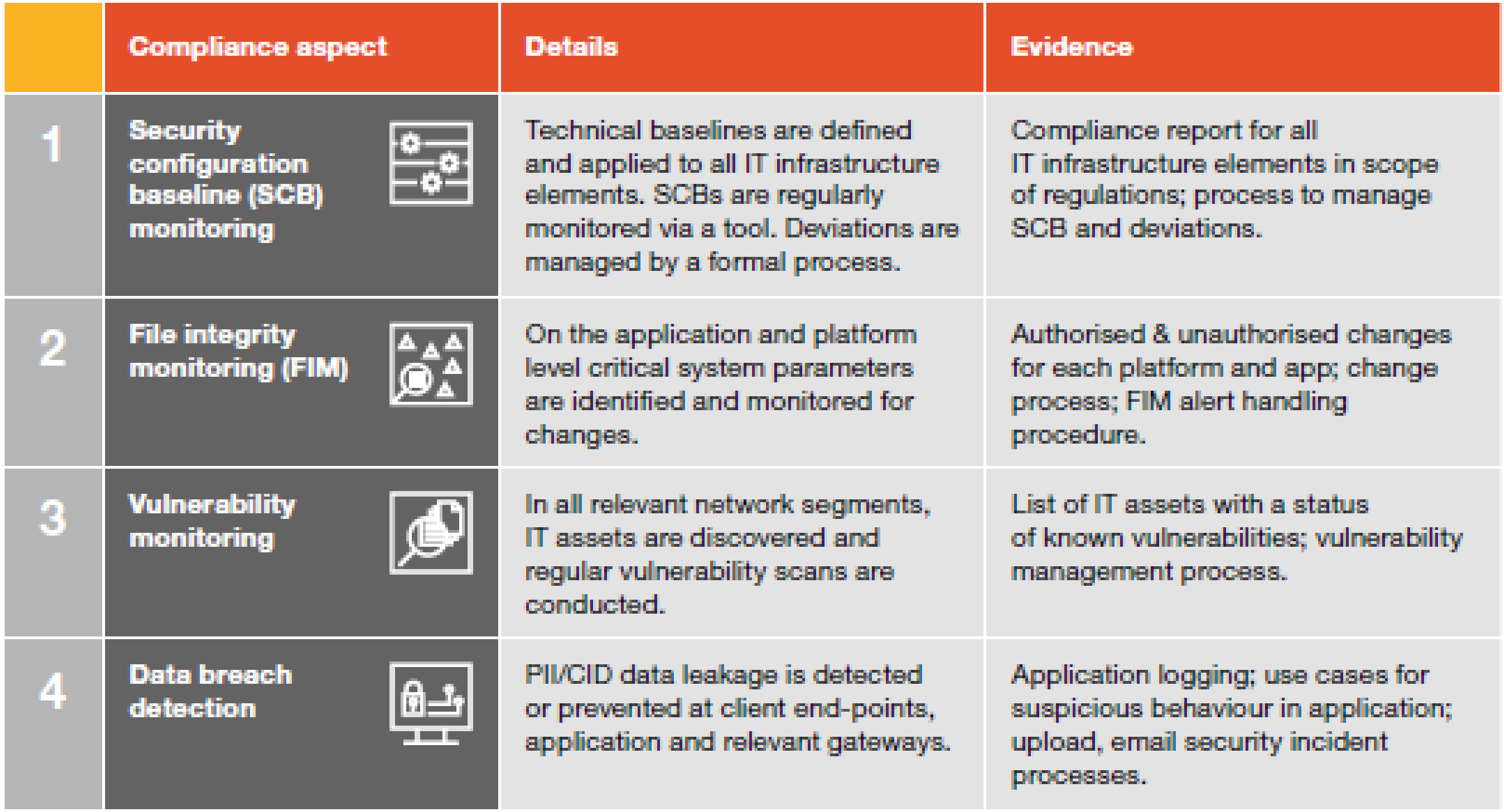
Typical Evidence for Audit



| View | Scan | Status | Date | Component | System |
|---|---|---|---|---|---|
| | 170 | NoChange | 2020/09/29 09:06:24 | AuthSystemLibs | SYSA |
| | 169 | NoChange | 2020/09/29 09:00:08 | AuthSystemLibs | SYSA |
| | 168 | NoChange | 2020/09/29 08:53:20 | ProdConfig | SYSA |
| | 167 | NoChange | 2020/09/29 08:52:44 | ProdConfig | SYSA |
| | 166 | NoChange | 2020/09/29 08:51:52 | ProdConfig | SYSA |
| | 165 | NoChange | 2020/09/29 07:02:26 | Monitor00010 | SYSC |
| | 164 | Correct | 2020/09/29 06:56:56 | App9:1.0.0 | SYSC |
| 👁 | 163 | Mismatch | 2020/09/28 11:50:13 | ProdSynch | SYSB |
| 👁 | 162 | Changed | 2020/09/28 11:50:01 | ProdSynch | SYSA |
| | 161 | Correct | 2020/09/28 08:42:32 | ProdSynch:Apr2019 | SYSC |

# Zero Trust - PWC

“An enterprise monitors integrity and security posture of all owned and associated assets. **No asset is inherently trusted**.” – NIST 2021



| | Compliance aspect | Details | Evidence |
|---|---|---|---|
| 1 | Security configuration baseline (SCB) monitoring | Technical baselines are defined and applied to all IT infrastructure elements. SCBs are regularly monitored via a tool. Deviations are managed by a formal process. | Compliance report for all IT infrastructure elements in scope of regulations; process to manage SCB and deviations. |
| 2 | File integrity monitoring (FIM) | On the application and platform level critical system parameters are identified and monitored for changes. | Authorised & unauthorised changes for each platform and app; change process; FIM alert handling procedure. |
| 3 | Vulnerability monitoring | In all relevant network segments, IT assets are discovered and regular vulnerability scans are conducted. | List of IT assets with a status of known vulnerabilities; vulnerability management process. |
| 4 | Data breach detection | PII/CID data leakage is detected or prevented at client end-points, application and relevant gateways. | Application logging; use cases for suspicious behaviour in application; upload, email security incident processes. |

**PWC –Zero Trust** https://www.pwc.ch/en/publications/2020/ch-zero-trust-whitepaper-final.pdf

# FIM+ can help you

- Auto-Discover sensitive components (zero admin)
- Detect changes that bypass existing tools (internal threats)
- Respond to incidents faster – automated detection / forensics
- Eliminate false alarms & redundant effort
- Comply with specific aspects of Zero Trust, PCI, NIST, Cyber Resiliency
- Allow staff to make the right decisions, with all the facts in one place
- Run all on mainframe, or feed your enterprise security console

Mainframes are high value targets – Defend them properly

# Wrap Up and Questions

Talk to an expert

- Deeper Dive
- Discuss specific needs

Do an express trial

- Free, takes a couple of days
- Auto-Discover APF and other sensitive datasets
- Run a full test suite – ours and yours
- Keep the Whitelist that the system builds

Hackers are moving ahead – Are you?

Call us at (403) 818-8625 or info@MainTegrity.com