Virtual IMS user group: Newsletter 79

Welcome to the Virtual IMS user group newsletter. The Virtual IMS user group at itech-ed.com/virtualims is an independently-operated vendor-neutral site run by and for the IMS user community.

Virtual IMS user group presentation

The latest webinar from the Virtual IMS user group was entitled, “Making IMS the most secure system on the planet”. It was presented by Al Saurette, VP Business Development, and Gary Euler, Consultant, at MainTegrity Inc.

Al is a principal at MainTegrity Inc and is dedicated to improving security on mainframes and other platforms. For over 35 years, he has delivered innovative solutions for enterprise IT problem areas. With a strong Operations background, he is a regular speaker at international security conferences and has authored many IT industry thought-leadership papers.

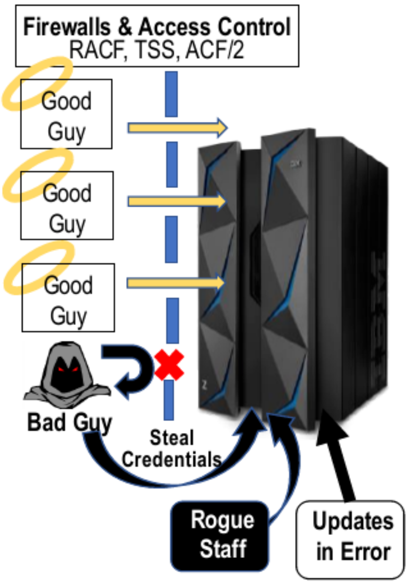


Figure 1: The security need

During his over 35 years in the IT industry, Gary has held senior management positions in a variety of IT companies that were engaged in both software development and IT services. Gary has held senior positions as a technician including as an IMS Systems Programmer,

Contents:

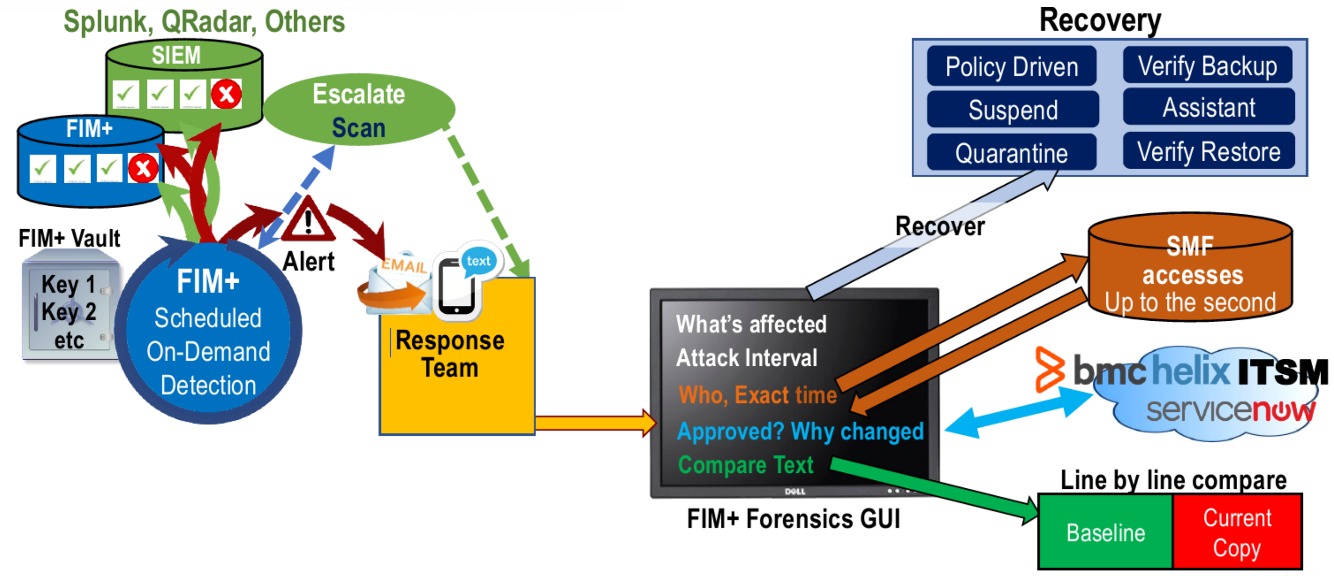


Figure 2: Manage, Detect, Respond, Recover

as a senior manager in IT delivery, and in a variety of business development roles.

Gary Euler started off by looking at the rise of the hacker from a lone wolf hacking for fun through to organized crime and nation state attacks.

Gary then gave use some statistics about mainframes, ATMs, and IMS:

- There are $7.7 trillion credit card payments (annual).
- There are 29 billion ATM transactions (annual).
- That's 12.6 billion transactions (daily).
- 87% of credit card transactions are performed on z/OS.

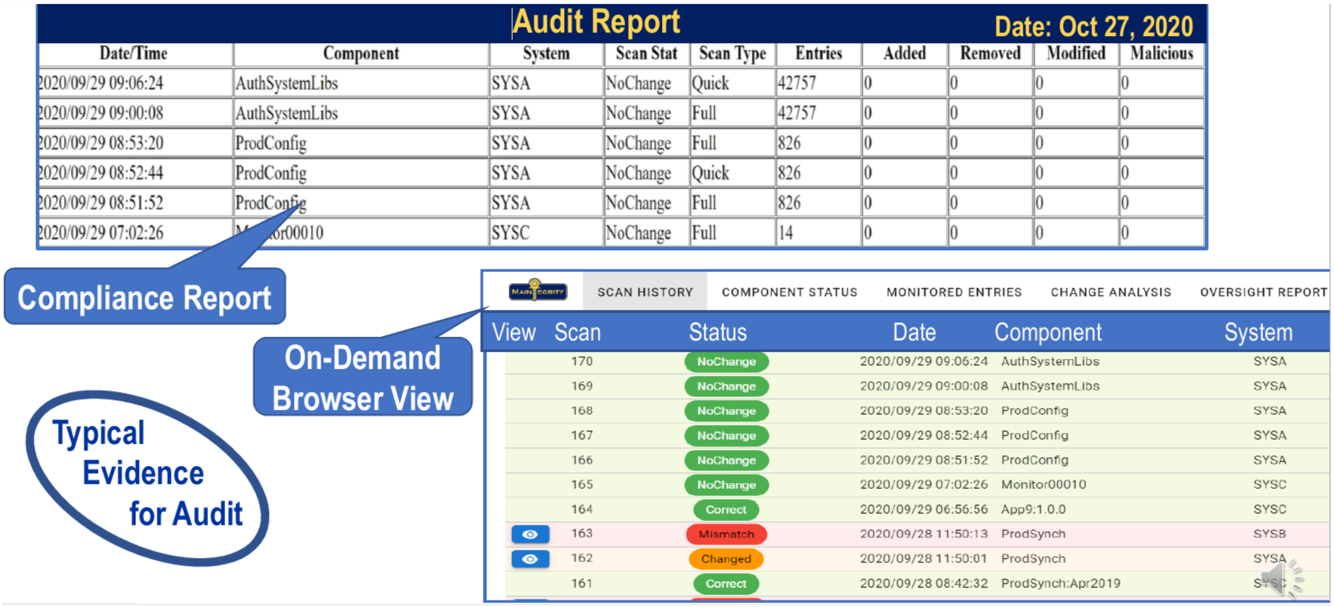
At the same time, the IT world is increasingly unsafe. The dark web has many millions of userid / passwords for sale. Organized crime and nation states are increasingly involved. And that's resulting in governments calling for 'zero trust' cyber infrastructures.

Figure 1 illustrates that bad actors can use stolen credentials to get through your perimeter, and rogue staff are not affected by firewalls and access controls. As Forrester says, 'Perimeter security has failed".

A simple Google search turns up an impressive array of z/OS hacking tools. There are Z/OS System Enumeration Scripts like: ENUM, which displays APF datasets, catalogs, RACF information, and all SVCs; STARTMAP, which displays IPL information and proclibs; CATMAP, which walks a catalog and gathers PDS and PDSE member names; and SYSOWN, which lists libraries and the meta data of the files in this TSO session.

There are also multipurpose NMAP scripts, TPX Brute (a z/OS TPX logon panel brute forcer), RACF database parser, and mainframe application pentesting software like CICSpwn and BIRP.

The steps in an advanced ransomware attack are: **reconnaissance**, where the hackers find out about an organization; **penetration**, where through phishing attacks that install keyloggers, or through the



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

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

Figure 3: Proof of compliance

purchase of userids and passwords from the dark web they are able to penetrate your mainframe; **fortify** their attack by leaving copies of code in case they are found; **infiltrate** your data and backups and take copies; **spoliation** where your data (including backups) is encrypted or corrupted; and you get a **ransom demand**.

In order to create a z/OS data fortress, a FIM+ (file integrity monitoring) solution provides:

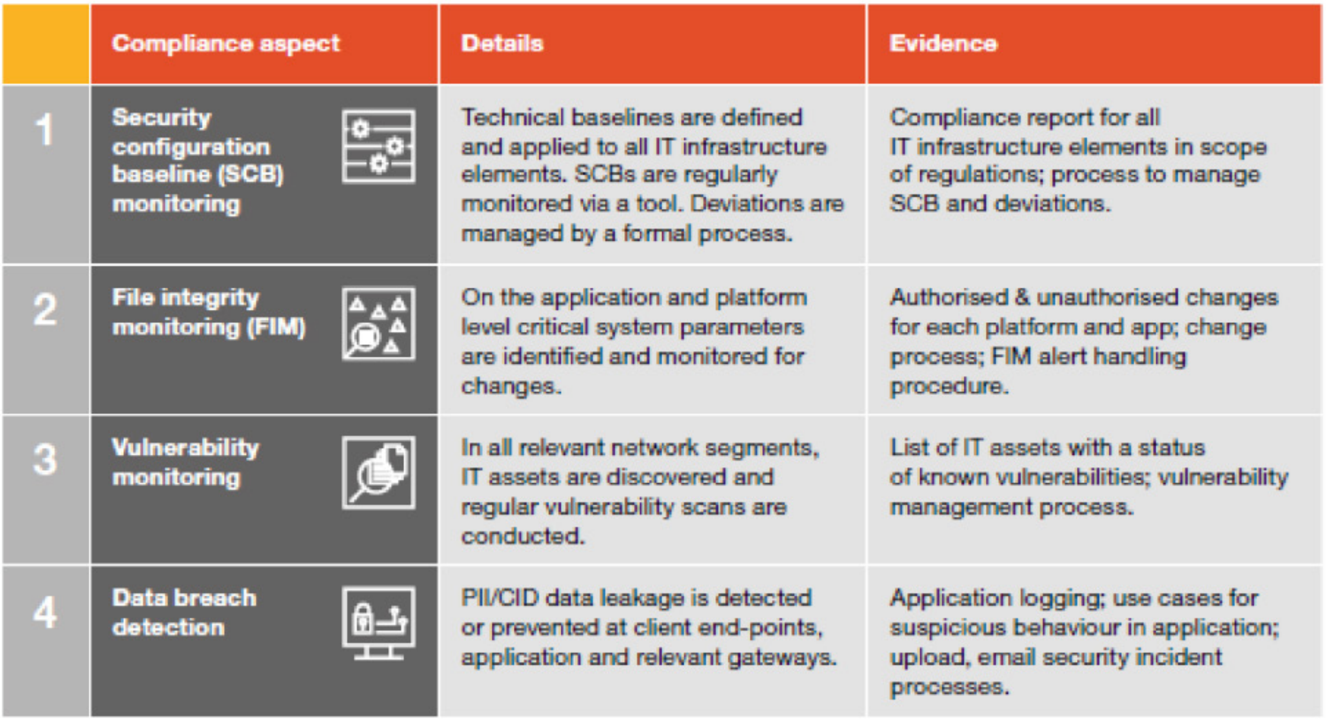
- Whitelisting, FIM+ discovers/monitors key elements
- Integrity verify backups, using a checksum
- Real-time access and FIM alerts via email / text
- Forensic data gathering / display using SMF, approvals
- Policy driven actions: including file quarantine, deletion, and guilty userid suspension
- Audit records to prove compliance with PCI, NIST, GDPR.

Figure 2 illustrates how FIM+ can manage, detect, respond, and recover. Al Saurette described in detail how that worked. He described how the software could identify your data, and keep a baseline record in a vault. And how it could then identify any changes. Those changes could be checked to see whether they were authorized. And, if not, alerts could be immediately sent out. The software could also remediate the situation following the corporate policies laid down.

Al highlighted that by using FIM+, not only could ransomware attacks be identified very quickly, they could also be prevented from spreading, and fixed. And this could be done at light speed compared to trying to resolve the issue without FIM+.

He summarized by saying that FIM+ will verify backups, send early warnings, provide real-time alerts, react quickly and forensically, scope out what else was affected, and prevent a ransom attack.

Al then turned his attention to compliance, particularly the Payment Card Industry



	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.

Figure 4: Zero-trust guidelines from PWC

Data Security Standard. He said that section 10.5.5 asks: “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)?”. And section 11.5 asks: “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?”. Even though your CIO, CFO, or CEO signs the section 3 validation form, most mainframe sites probably aren’t currently compliant with the regulations.

Next, Al highlighted last year’s ATM cash-out attack, where thieves breached bank’s or card processor’s security to manipulate fraud detection and they took lots of cash from a number of ATMs. The key points in the attack were that most ATM transactions are captured by IMS on a mainframe. The card management system was altered, ie changes to parameters or executables were made. And that takes knowledge and coordination. It was most likely an ‘inside job’.

The recommended best practices were:

1 24/7 monitoring with File Integrity Monitoring (FIM)

2 Improved detection, response, and recovery

3 Strict separation of roles, ie no ‘inside jobs’.

Al also mentioned that FIM+ produces the necessary evidence of compliance required by auditors (see Figure 3).

Zero-trust seems to be the way that security is going. NIST in 2021 said: “An enterprise monitors integrity and security posture of all owned and associated

Our website is:

itech-ed.com/virtualims

assets. No asset is inherently trusted." PWC recently published some guidelines (see Figure 4) and these highlight the pivotal role played by file integrity monitoring.

Al wound up the presentation by saying that FIM+ can help an organization using a mainframe:

- Auto-discover sensitive components (zero admin)
- Detect changes that bypass existing tools (internal threats)
- Respond to incidents faster with automated detection / forensics
- Eliminate false alarms and 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 it all on the mainframe, or feed your enterprise security console.

A copy of Al Saurette and Gary Euler's presentation is available for download from the Virtual IMS user group Web site at itech-ed.com/virtualims/presentations/IMSFIMJun21.pdf.

You can see and hear the whole user group meeting at https://youtu.be/IDDiZM6Q7aE.

Meeting dates

The following meeting dates have been arranged for the Virtual IMS user group:

- On 10 August, Dougie Lawson will be discussing "From Legacy to Infinity & Beyond".
- The following meeting will be on 12 October, when Karen N Tischer, dba IMS Education & Consulting, Instructor/Consultant will be giving an "Overview of Fast Path DEDBs".

About the Virtual IMS user group

The Virtual IMS user group was established as a way for individuals using IBM's IMS hierarchical database and transaction processing systems to exchange information, learn new techniques, and advance their skills with the product

The Web site at https://itech-ed.com/virtualims provides a central point for coordinating periodic meetings (which contain technically-oriented topics presented in a webinar format), and provides articles, discussions, links, and other resources of interest to IBM IMS practitioners. Anyone with an interest in IMS is welcome to join the Virtual IMS user group and share in the knowledge exchange.

To share ideas, and for further information, contact trevor@itech-ed.com.

The Virtual IMS user group is free to its members.