Virtual IMS user group: Newsletter 74

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.

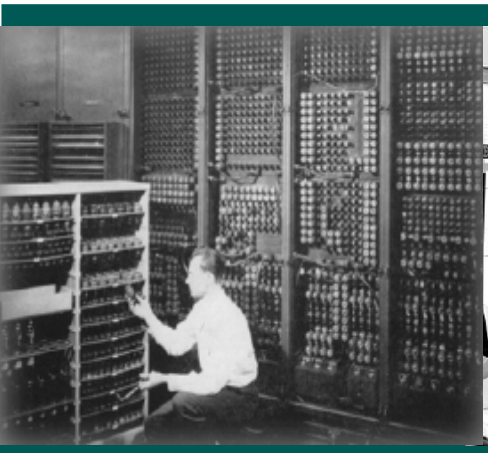
Figure 1: How secure is my mainframe?

Virtual IMS user group presentation

The latest webinar from the Virtual IMS user group was entitled, "Implement IMS Analytics for Better Business Outcomes". It was presented by Nick R Griffin, WorldWide IMS Specialist at BMC.

Nick has over 40 years of mainframe experience in Development, Systems, and Database Administration for IMS, MVS, CICS/VSAM, and VTAM applications. Nick has been a developer for IMS Monitoring code and managed a development group for a competitive

Contents:



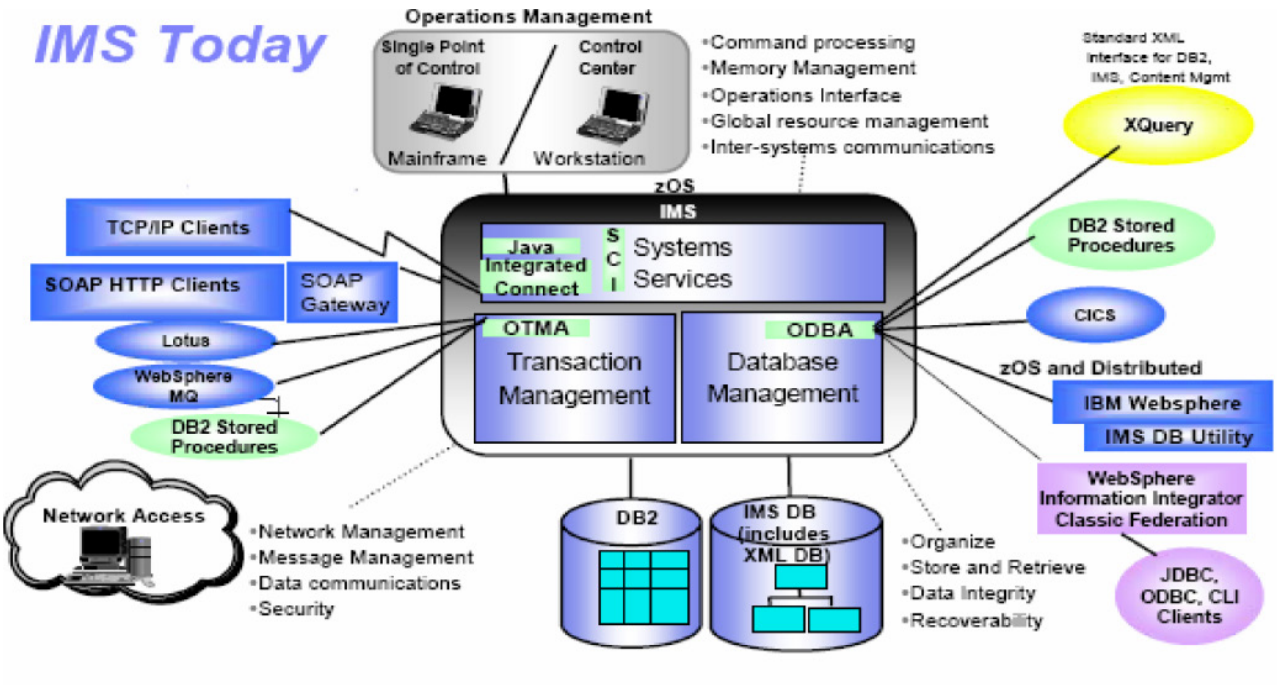


Figure 2: IMS connectivity

software vendor. Nick managed large, complex, mission-critical IMS database applications for a variety of Fortune 500 companies. Most recently, he has spent 14 years as IMS Product Manager for a large tools vendor. Nick is currently assisting sales as IMS Product Account Manager.

Nick started his presentation by looking at mainframe security (see Figure 1). He gave a number of reasons why mainframers often feel their mainframe is secure, eg:

- We passed a compliance audit, so everything must be secure
- The mainframe can't be hacked
- Event logs would show any security issue or threat of intrusion immediately.

He went on to say that the truth is:

- The mainframe is closer to the Internet, applications, and credit card information – the data that hackers want – than ever before
- On average it takes ~200 days to detect a breach
- Have you ever tried looking at an IMS log?

Nick confirmed that the mainframe can be hacked. In 2008, Luxottica, the parent company of LensCrafters, suffered a mainframe breach exposing nearly 60,000 employees' records from its US headquarters. In 2013 the mainframes of Logica and the Swedish Nordea Bank were hacked. And there have been other, more recent, attacks.

Nick recommended using SIEM (Security Information and Event Management) systems, which have long been the industry standard for enterprise network security for distributed platforms.

Nick then gave the user group some statistics about

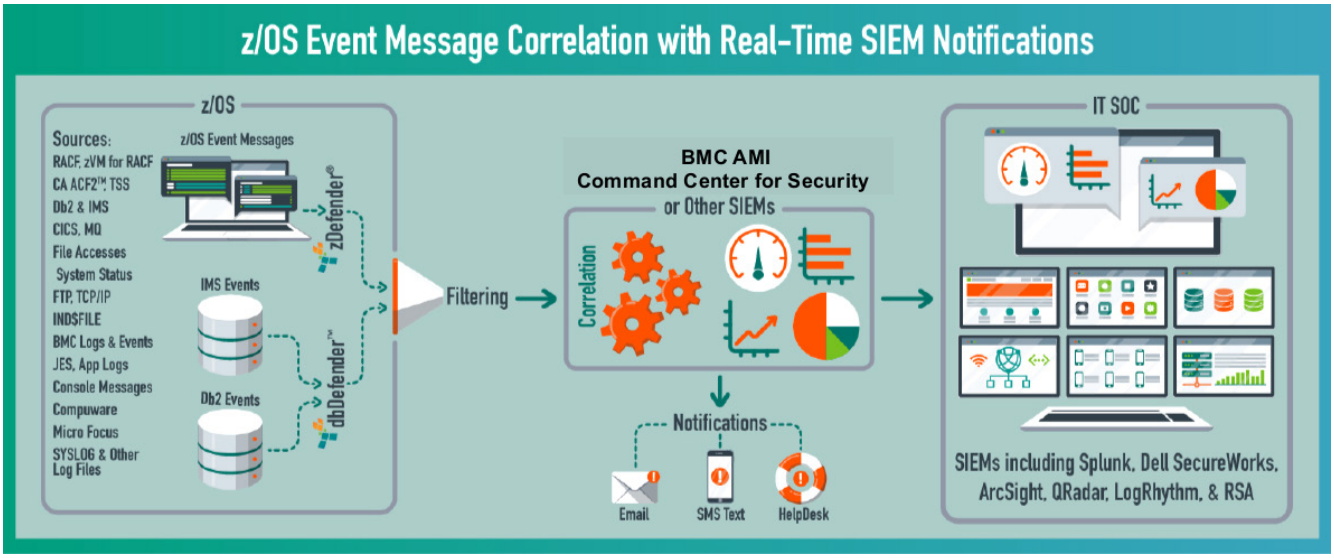


Figure 3: AMI for Security architecture

breaches, saying that it took, on average, 197 days to identify a breach. And the average total cost of a breach to a US company is $7.9 million.

According to BMC's Mainframe Survey: security is consistently ranked #2 in priority at 54 percent of sites; executives agree that data privacy/compliance/security is a top priority; and 34 percent of large shops are using Pervasive Encryption to ensure data security.

Nick suggested that without real-time mainframe event messages in your SIEM, IMS users have a mainframe security gap.

Nick Griffin explained that IMS was more connected than ever before (see Figure 2). It isn't just terminals that connect to it – and that increases the attack surface.

The other big issue is that IMS logs can be massive, which makes looking through them difficult and time consuming.

That's where products like AMI for Security come in because they offer real-time visibility and alerts that appear in the SIEM. The products that BMC has in this area are:

- BMC AMI Command Center for Security, which offers point-and-click functionality from a standard Web browser into z/OS security and operational events, and provides dashboard views, event message correlation, and notifications.
- BMC AMI Defender for z/OS, which expands the role of your corporate IT security system to include real-time mainframe messages to network security.
- BMC AMI Defender for Db2, which provides up-to-the-second data set monitoring and security alerts for event logs from Db2.
- BMC AMI Defender for IMS, which provides up-to-the-second user monitoring and security alerts for IMS events.

Nick then looked at the capabilities of BMC AMI for Security, and Figure 3 shows

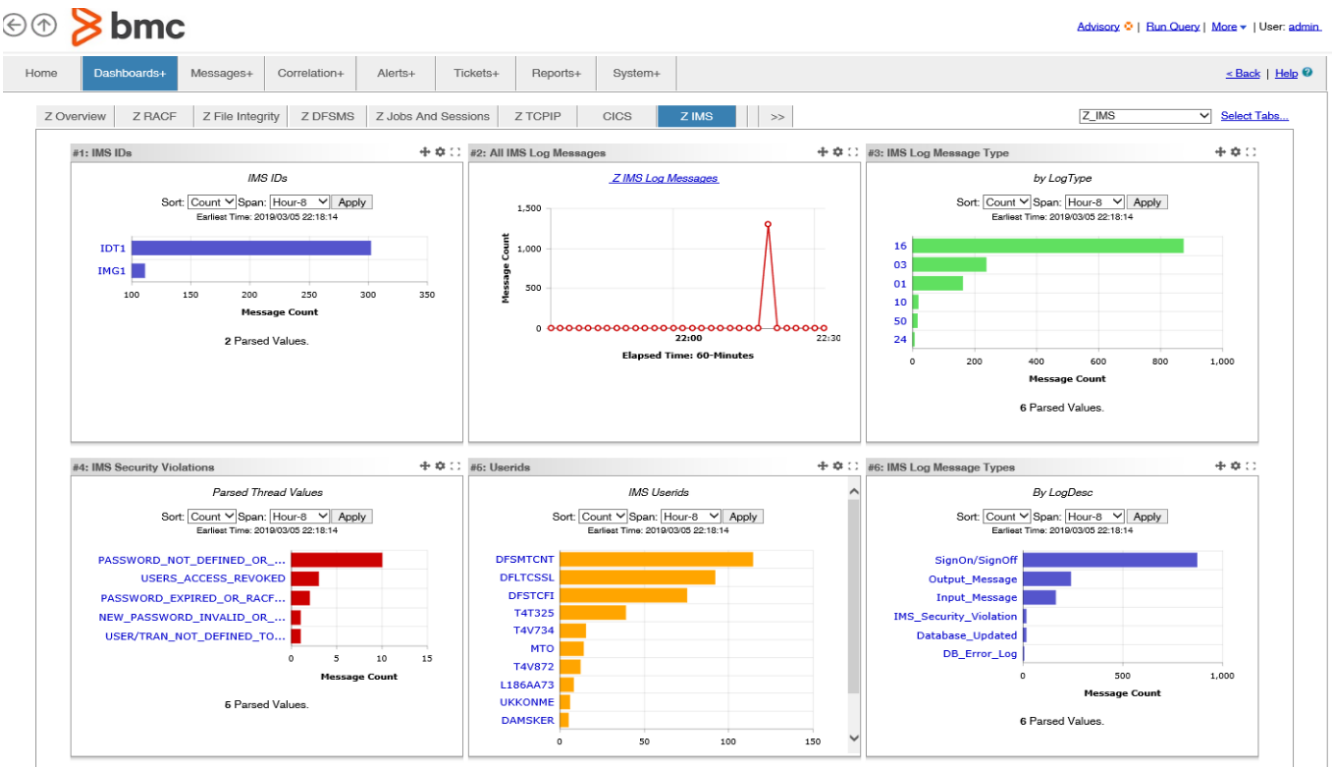


Figure 4: Example dashboard

the architecture of AMI for security. Nick also showed what the command center looked like. An example of the dashboard is shown in Figure 4.

Focusing on BMC AMI Defender for IMS, Nick said that it:

- Extracts real-time IMS log information for use in SIEM applications or analytics engines
- Uses proprietary techniques that dramatically reduce the overhead associated with data extraction
- Uses advanced filtering routines to minimize the amount of unnecessary data ingested into the target engines.

AMI Defender for IMS server gathers IMS data and uses intelligent filtering. It also has an API for other BMC products. It can then export to Analytics Engines, DASD, Syncsort Ironstream, IBM, etc, and produce useful business data.

It takes IMS data in real time including IMS database updates/access including any log record type and user information. It does this with minimal overhead and without interrupting the log.

Information from the IMS log is in near real time. It can export date at log switch time.

Nick then showed some examples of using intelligent filtering and extraction with the product.

He then went on to describe the new features in BMC AMI Defender for IMS V.3.0.01.

By way of conclusion, Nick Griffin said that mainframes are more connected, so they are more susceptible to security attacks. It's easy

Our website is:

itech-ed.com/virtualims

to miss the breaches in the expansive capacity and speed of the mainframe. Event logs may be massive, and data fields are overwhelming. The mainframe can be hacked, and IMS data can be compromised.

He suggested that IMS users should use efficient tools and facilities to capture the right data in a timely manner. They should take the potential threats seriously. And they should protect their business with intelligent analytics that detect events and patterns that could affect them.

A copy of Nick Griffin's presentation is available for download from the Virtual IMS user group Web site at itech-ed.com/virtualims/presentations/IMSanalytics20.pdf.

You can see and hear the whole user group meeting at https://youtu.be/9ukEU1m6qkc.

Meeting dates

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

- On 6 October, Dusty Rivers, Director, z Systems Software: IMS & CICS at GT Software will be speaking.
- The following meeting will be on 8 December 2020, when Thomas Esser, zSolutions Architect and Director, IMS Solution Advisors at Rocket Software will be discussing "Saving CPU time with IMS database administration".

Recent IMS articles

IMS Support for z/OS Workload Interaction Correlator by Sanjay Kaliyur on z Systems Developer Community (2 July 2020). You can find the article at https://developer.ibm.com/zsystems/2020/07/02/ims-support-for-z-os-workload-interaction-correlator/

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.