Implement IMS Analytics for Better Business Outcomes

Nick Griffin

IMS Product Account Manager

How Secure is my Mainframe?

Myths

- 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

Truth

- 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?

bmc

The Mainframe Can Be Hacked

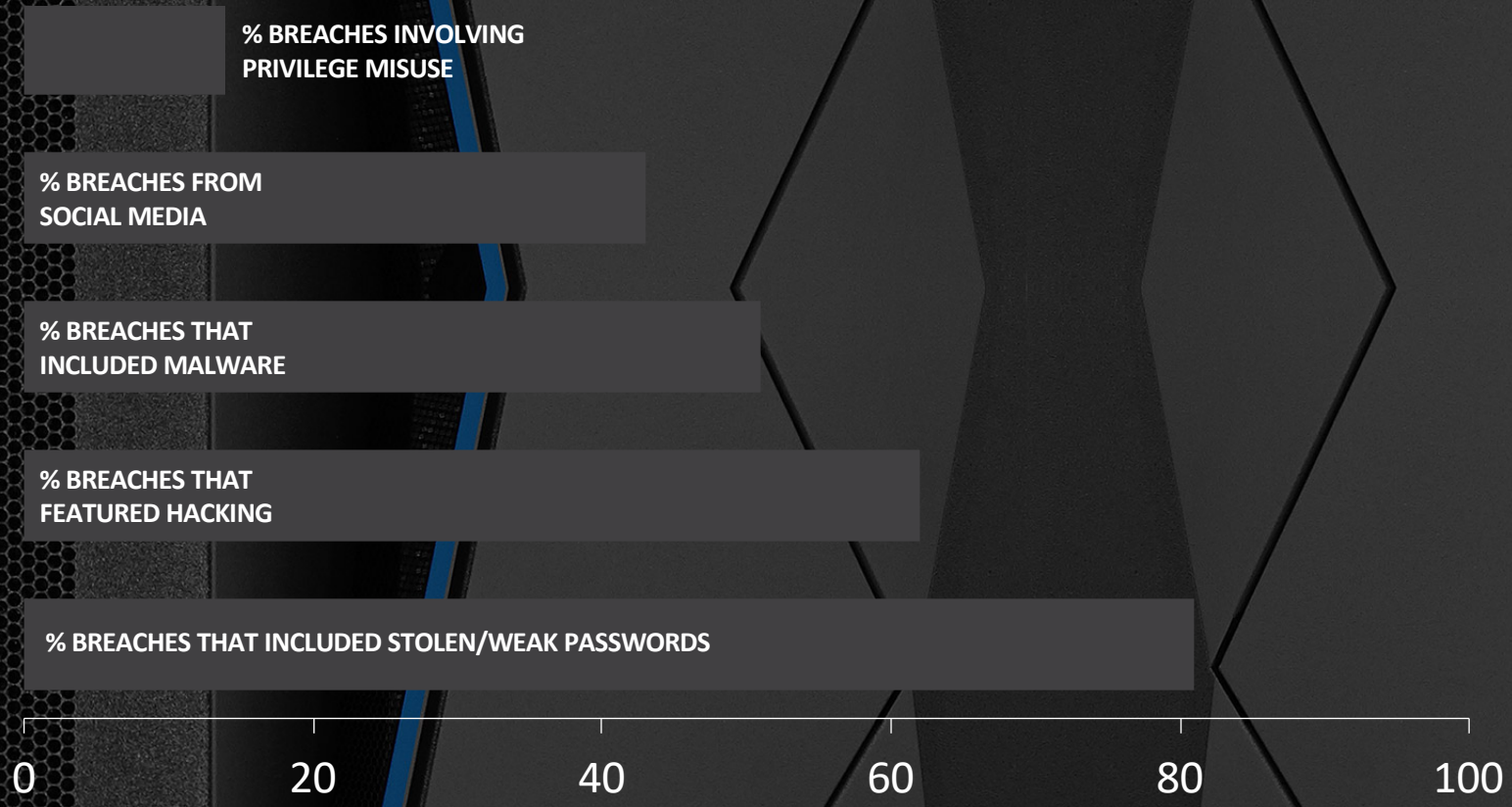
- SIEM (Security Information and Event Management) systems have long been the industry standard for enterprise network security, but the mainframe has mostly been left out of this predominantly distributed discipline.

2013 – Pirate Bay co-founder Gottfrid "anakata" Svartholm Warg hacked the mainframes of Logica and the Swedish Nordea Bank – allegedly from southeast Asia

2008 – Luxottica, the parent company of LensCrafters, suffered a mainframe breach exposing nearly 60,000 employees' records from its U.S. headquarters in Mason, Ohio – from an IP address in Glendale, Arizona

bmc

Breaches by the Numbers



Source: Verizon 2017 DBIR report

bmc

Breaches by the Numbers

197 Days — Mean time to identify breach

$7.9M — Average total cost of data breach in the US

$148 — Average cost per lost/stolen record

$408 — Average cost per lost record, per capita in healthcare

$206 — Average cost per lost record, per capita in financial

bmc

BMC's Mainframe Survey says…

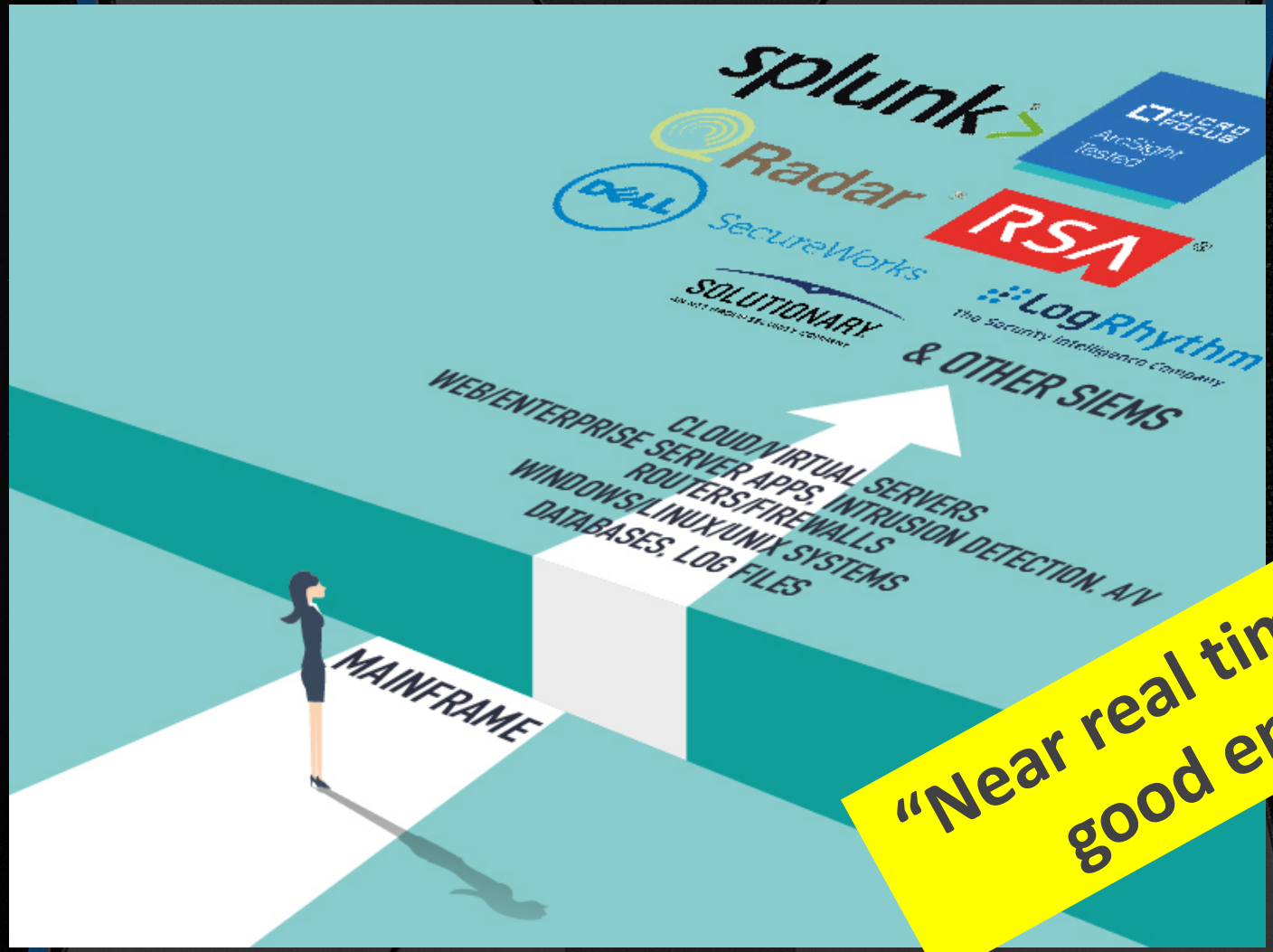
- Security is consistently ranked #2 in priority at 54%
- Executives agree Data Privacy/Compliance/Security is a top priority
- 34% large shops using Pervasive Encryption to ensure data security
-

bmc

“Every case involving cybercrime that I've been involved in, I've never found a master criminal sitting somewhere in Russia or Hong Kong or Beijing. It always ends up that somebody at the company did something they weren't supposed to do. They read an email, went to a website they weren't supposed to…”

Frank Abagnale, Jr.

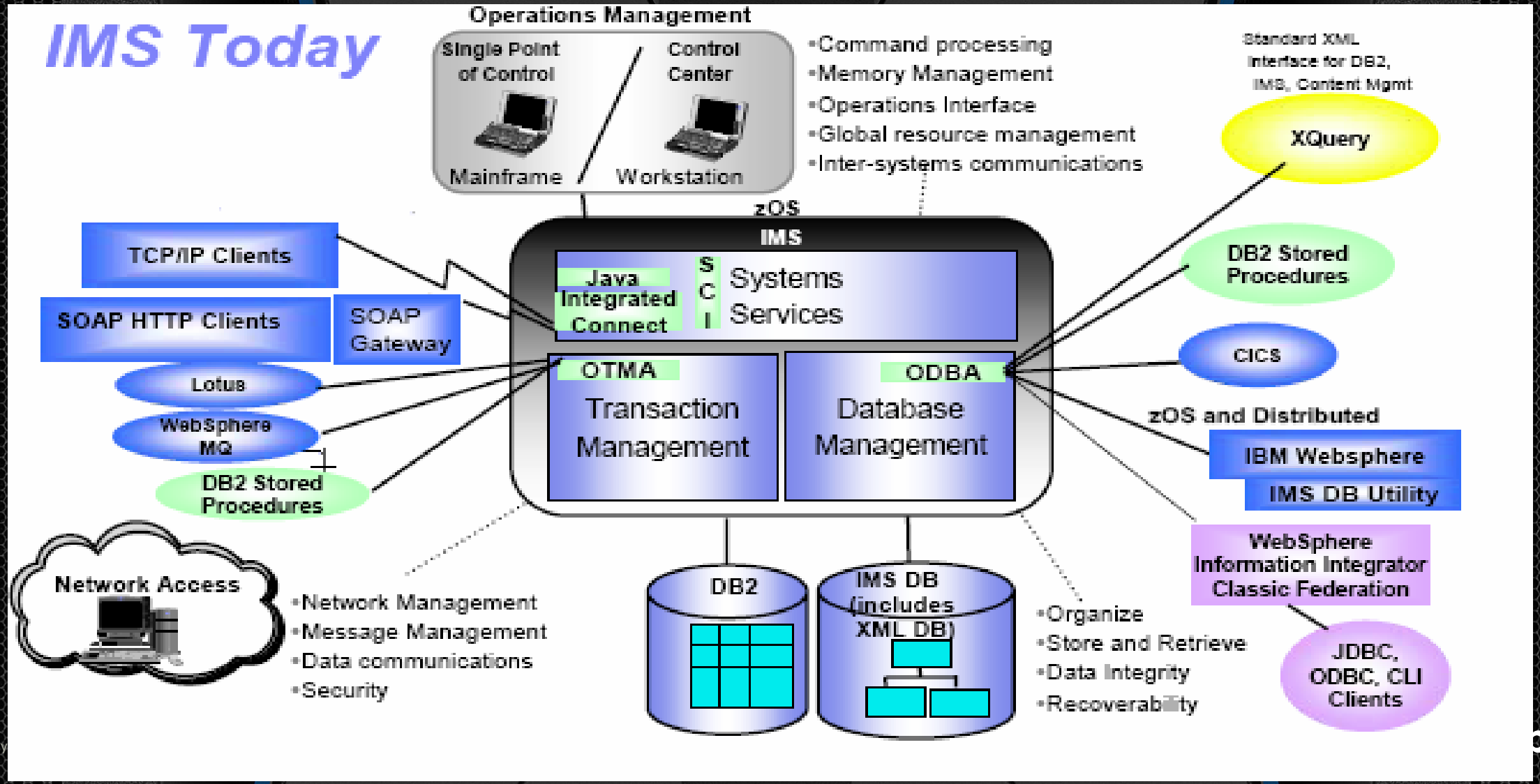
Without Real-time Mainframe Event Messages in your SIEM, You Have a Mainframe Security Gap



"Near real time" is not good enough!

bmc

IMS is more connected than ever



Not just terminals accessing IMS

IMS Logs can be massive

AMI for Security

Real-Time Visibility and Alerts

- BMC AMI Command Center for Security
  - Point-and-click functionality from a standard web browser into z/OS security and operational events
  - Dashboard views, event message correlation, and notifications
- BMC AMI Defender for z/OS
  - Expands the role of your corporate IT security system to include real-time mainframe messages to network security
- BMC AMI Defender for Db2
  - Up-to-the-second data set monitoring and security alerts for event logs from Db2
- BMC AMI Defender for IMS
  - Up-to-the-second user monitoring and security alerts for IMS events

Real time mainframe user events in your distributed SIEM

BMC AMI for Security Capabilities

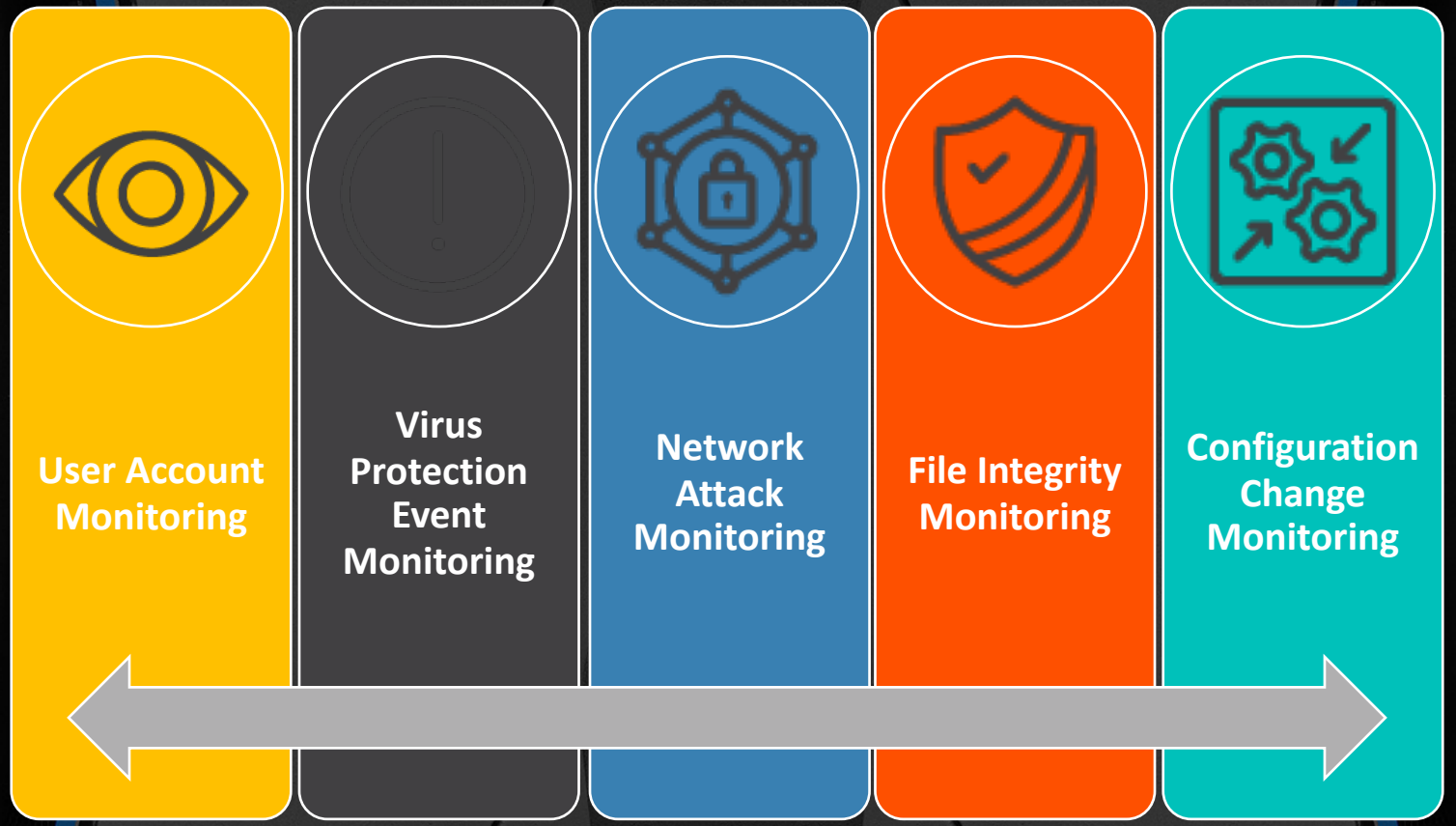
NERC

ISO 27001

GLBA

PCI DSS

FISMA



GDPR

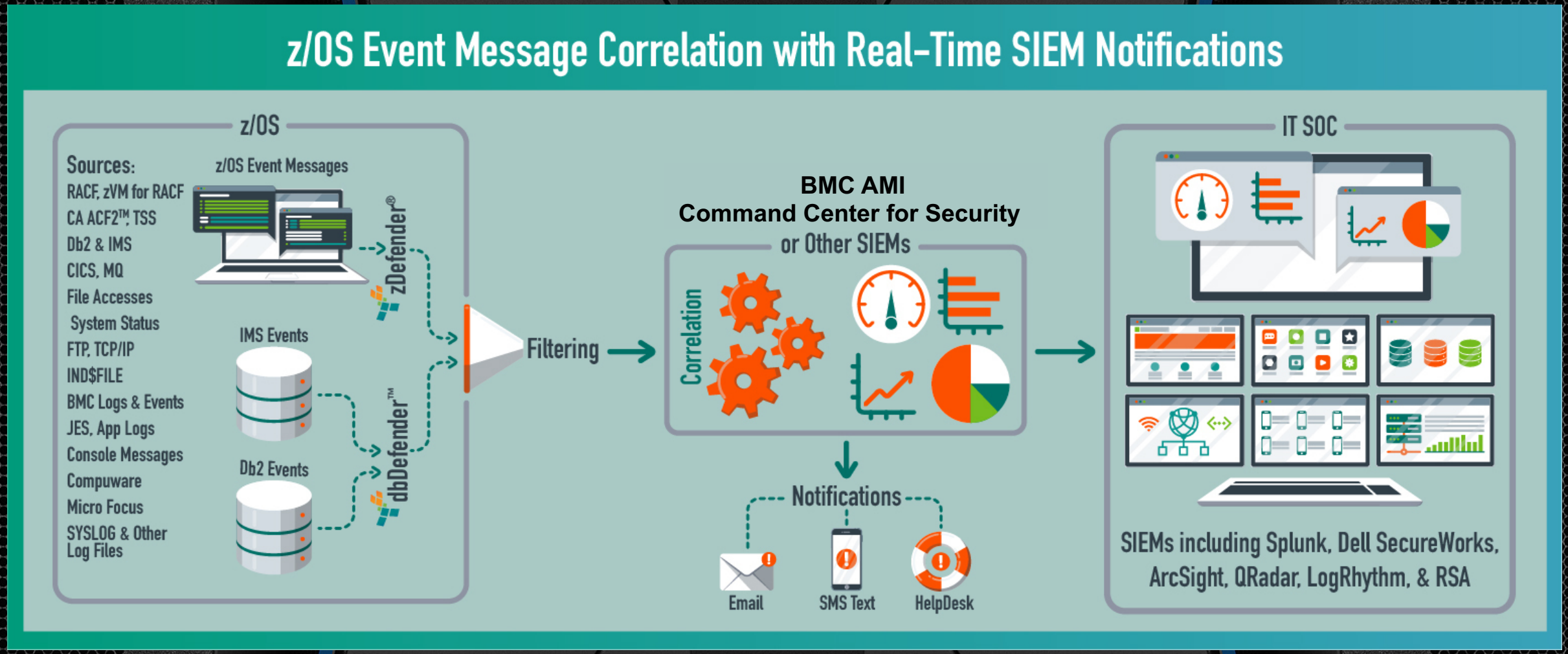
IRS Publication 1075

SOX

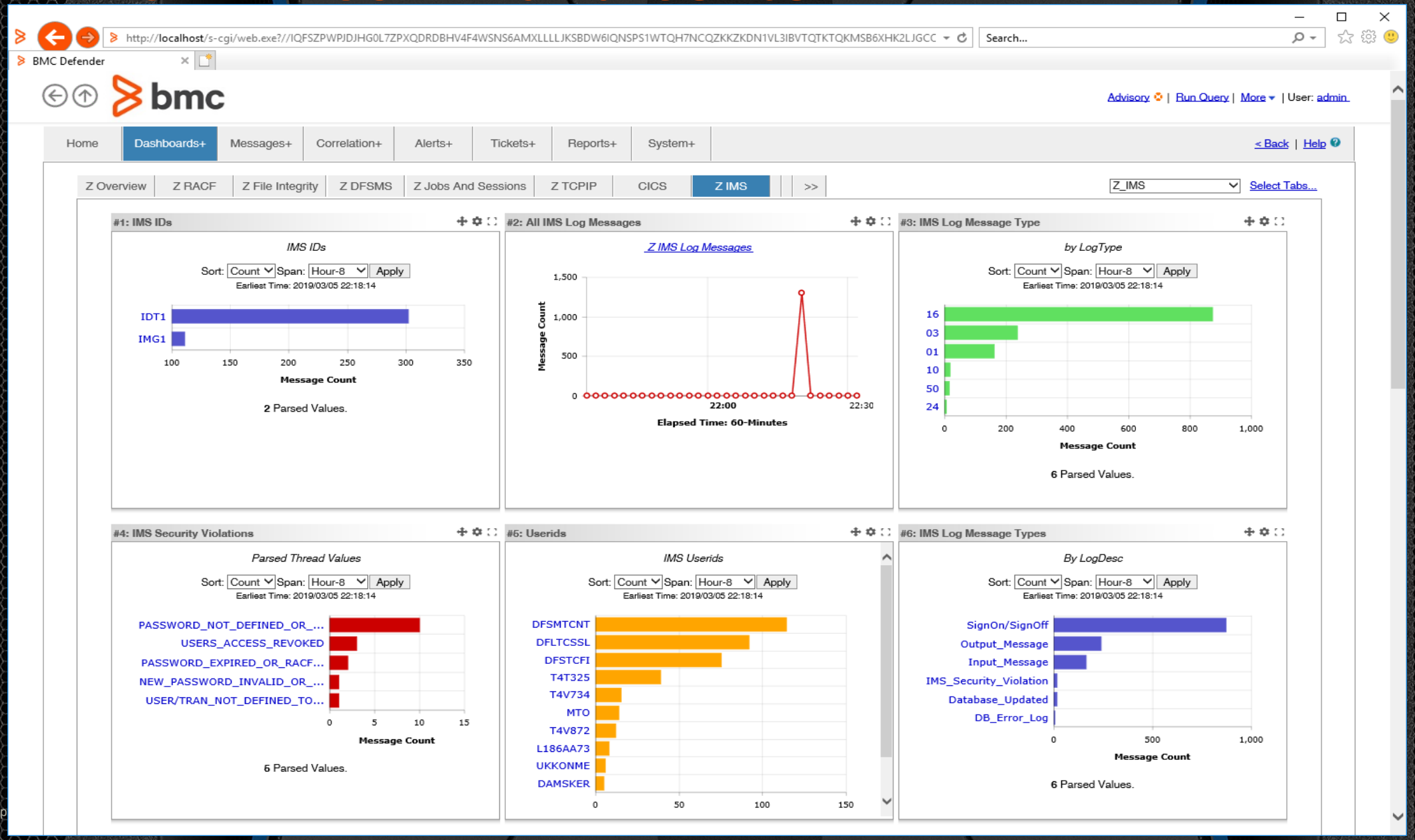
HIPPA

bmc

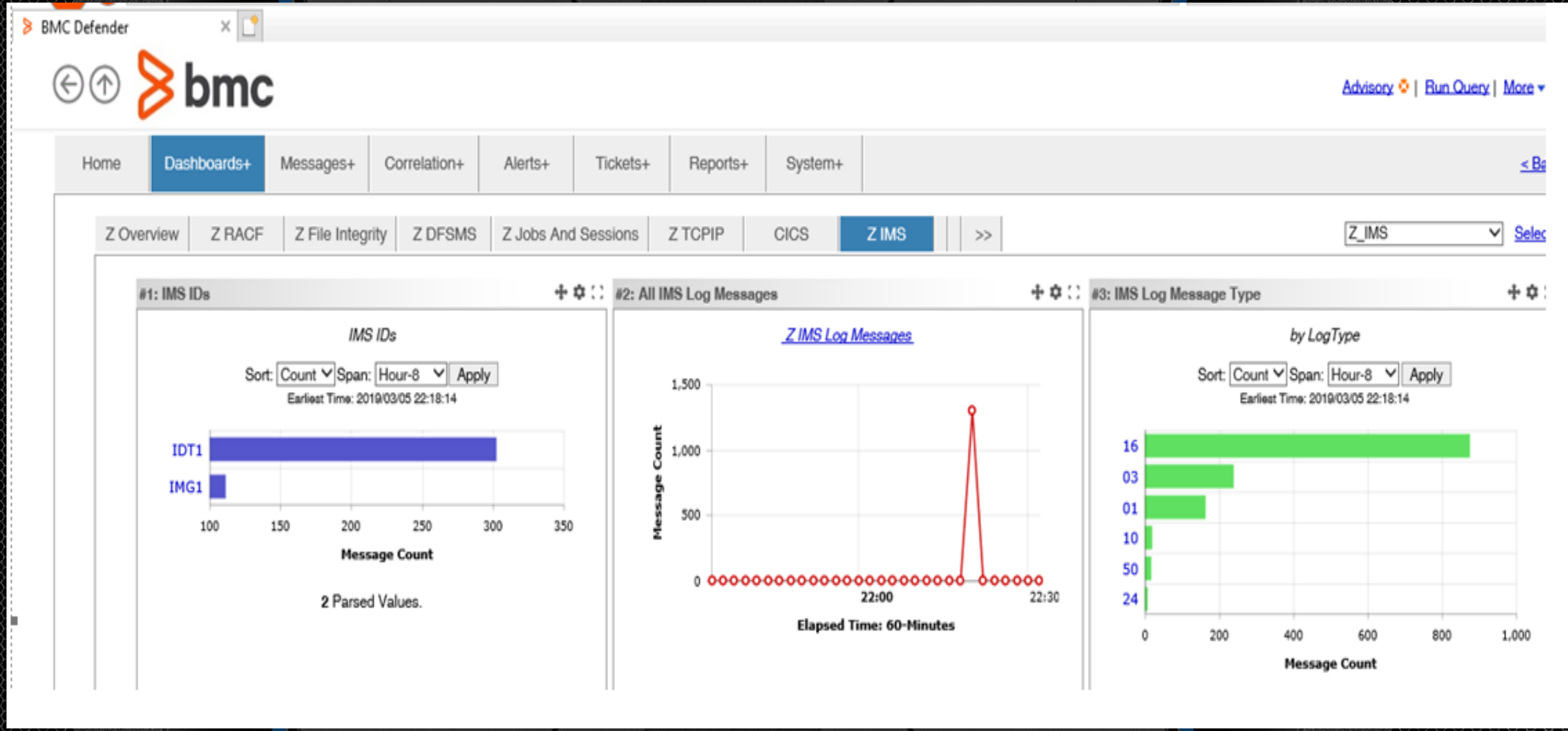
AMI for Security Architecture



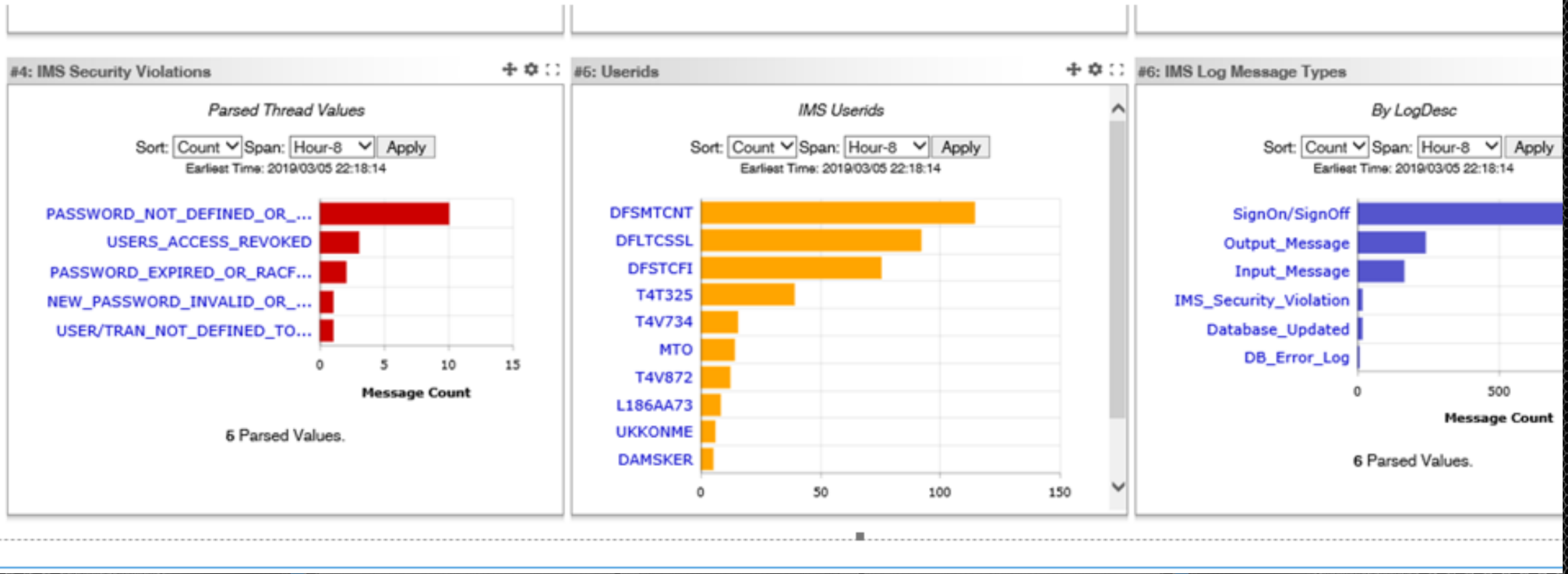
BMC AMI Command Center



BMC AMI Command Center



BMC AMI Command Center



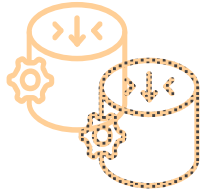
BMC AMI Defender for IMS

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

Mainframe Data Extraction Providers

IMS DATA

REAL TIME
IMS specific
IMS Database updates/access
Any log record type (i.e.1&3)
User information
Minimal overhead
No log interruptions



IMS LOG

NEAR REAL TIME
Exports data @ log switch time switch time will vary

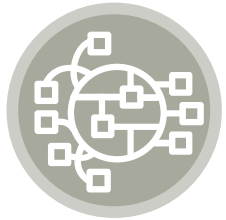
SYSTEM DATA
SMF Records
z/OS Sys Logs
"MAINVIEW" Data
Job Logs
Machine Data

syncsort

Ironstream

IBM

REAL TIME MAINFRAME DATA



AMI Defender for IMS server
Gathers IMS Data
INTELLIGENT FILTERING
API for other BMC products
Export to Analytics Engine, DASD, Syncsort Ironstream, IBM, etc.
Business Data

Analytics Engines

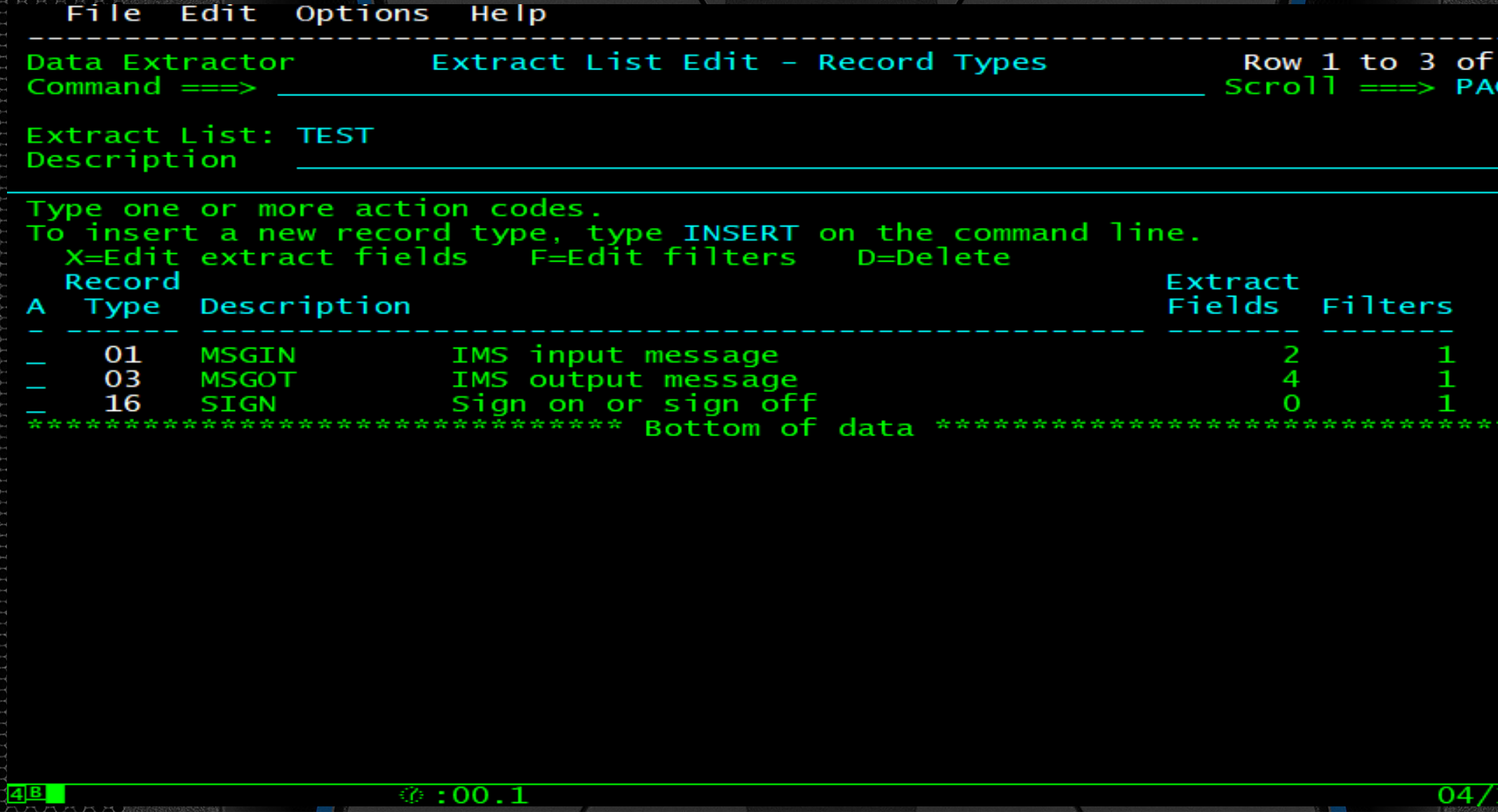
bmc

splunk>

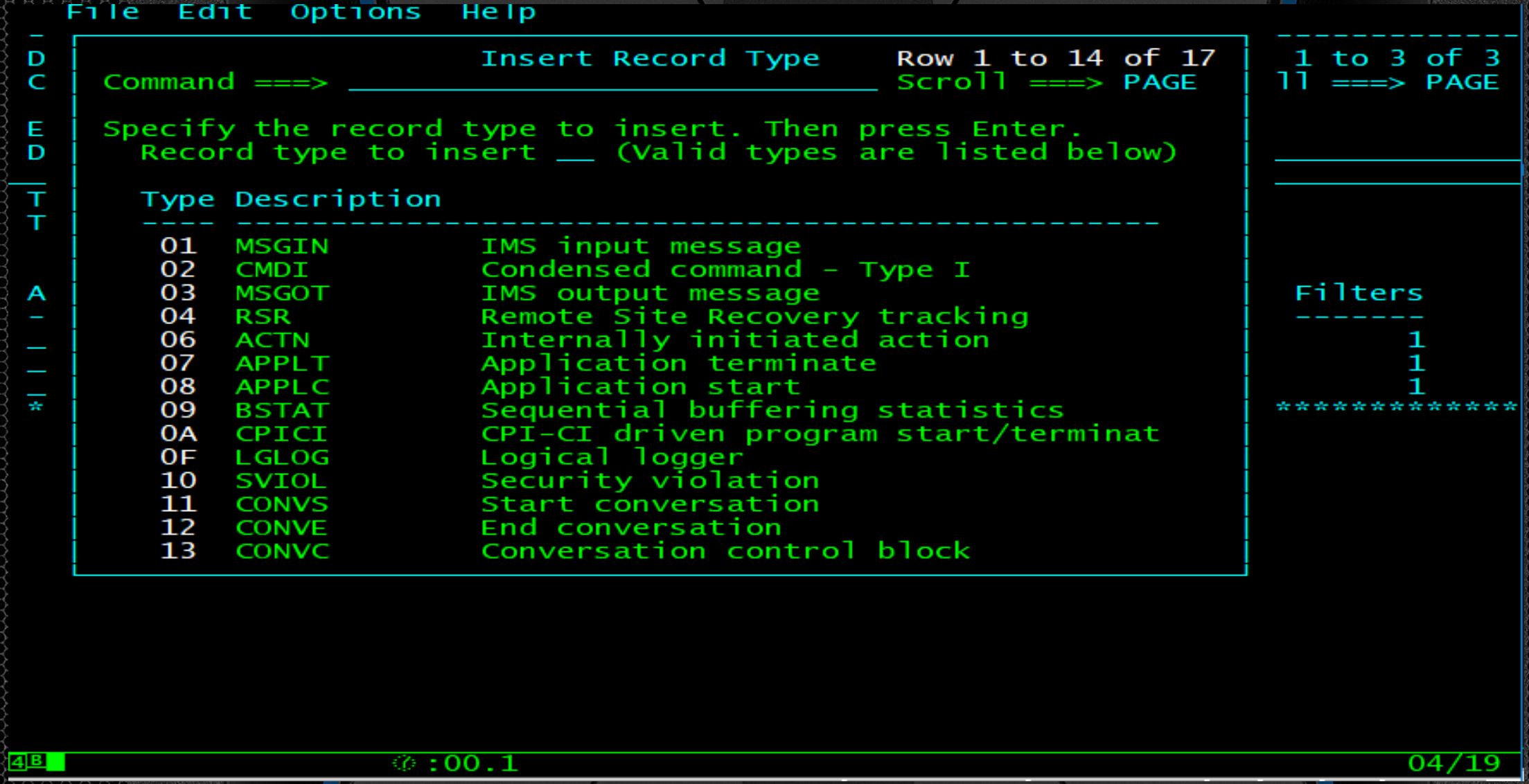
hadoop

APACHE Spark™

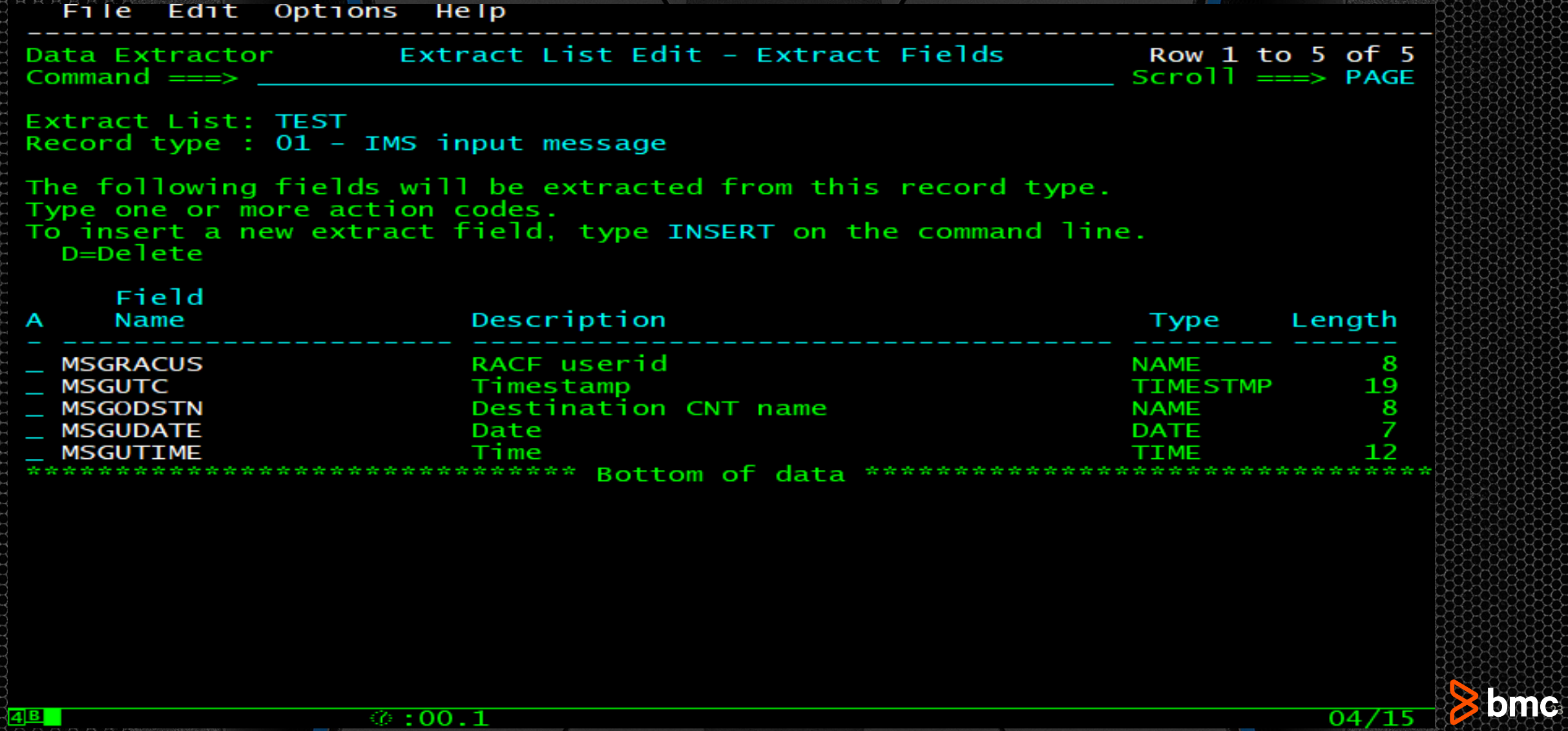
Intelligent filtering and extraction



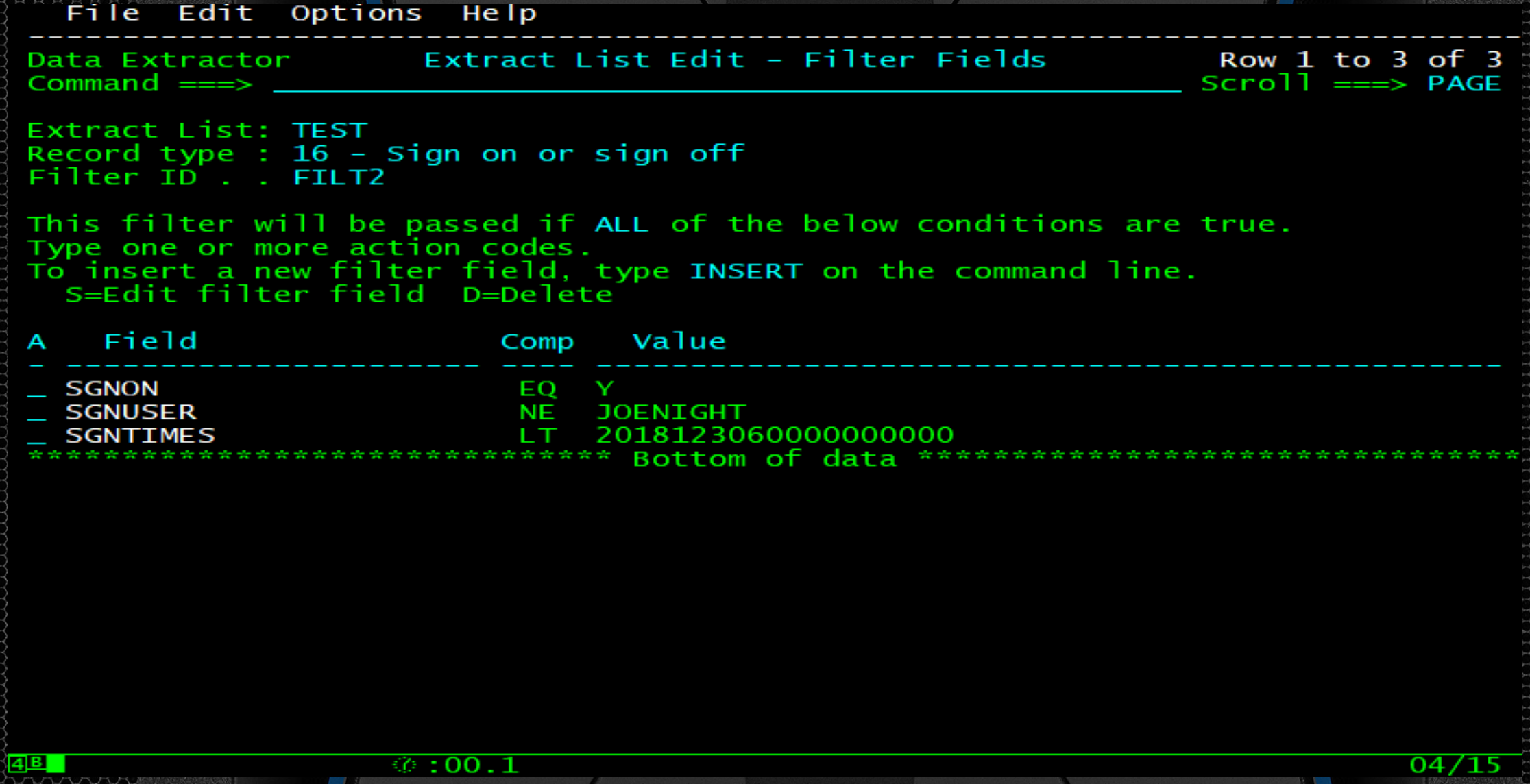
Intelligent filtering and extraction



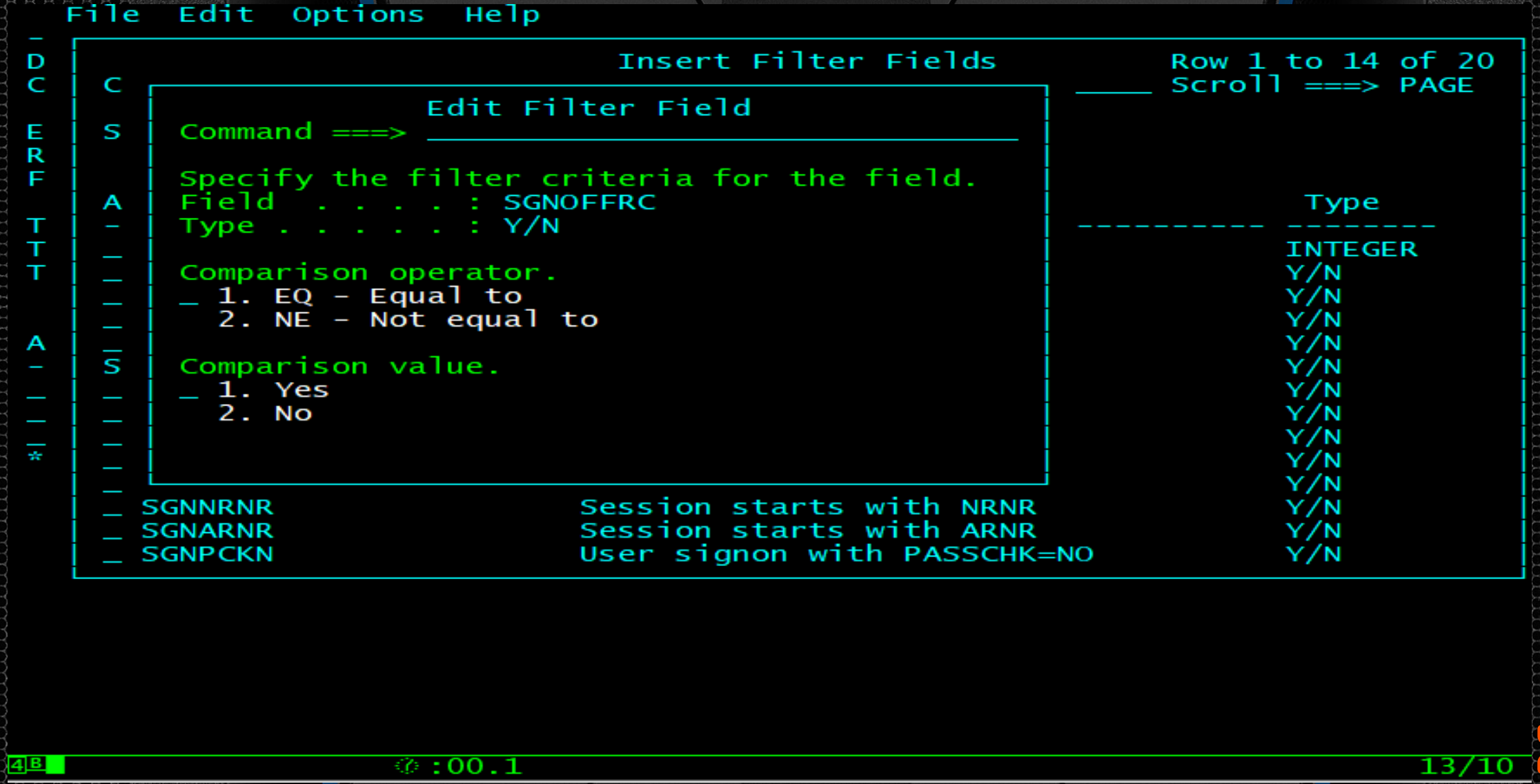
Intelligent filtering and extraction



Intelligent filtering and extraction



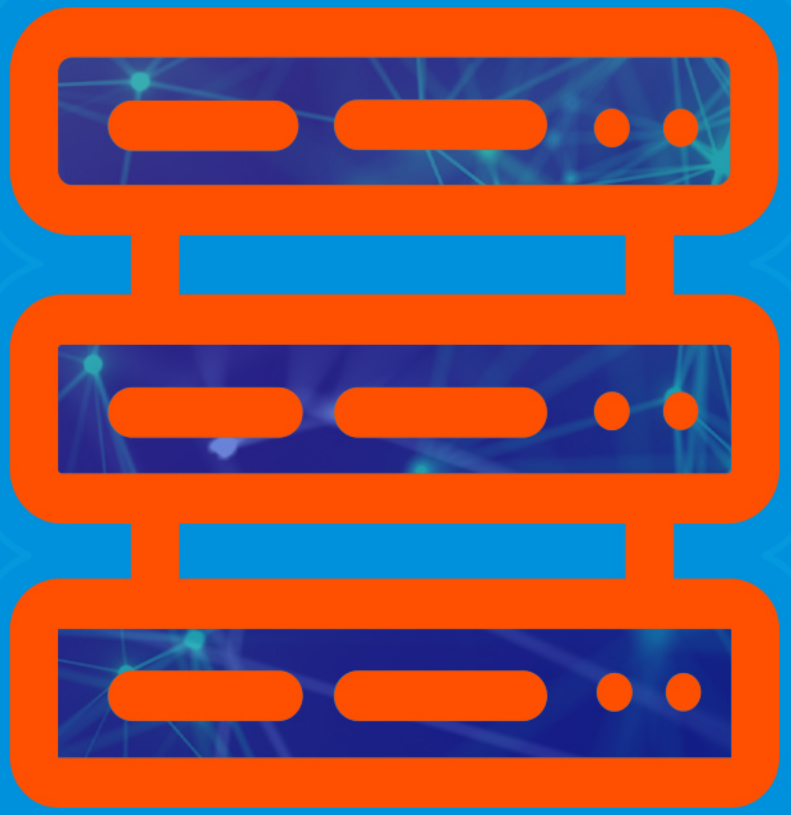
Intelligent filtering and extraction



Output from Realtime Log Capture


```
{"MSGUOW1":"X15APPL D5B90B0F3ECC7B91","MSGIDSTN":"ASDF    ","MSGODSTN":"ASDF    ","MSGXDATA_ALL":".","MSGXDATA_ALL_LEN":"00005","MS
{"MSGUOW1":"X15APPL D5B90B1500438186","MSGIDSTN":"ASDF    ","MSGODSTN":"IVTCV   ","MSGXDATA_ALL":"..IVTCV   .&.......    DIS
{"MSGUOW1":"X15APPL D5B90B15F4735996","MSGIDSTN":"        ","MSGODSTN":"DFSA1CNT"}
{"MSGUOW1":"X15APPL D5B90B1500438186","MSGIDSTN":"ASDF    ","MSGODSTN":"ASDF    ","MSGXDATA_ALL":"..IVTCV   .&.. ...DIS.. .ME.. .NO
{"MSGUOW1":"X15APPL D5B90B3290E3EB80","MSGIDSTN":"        ","MSGODSTN":"DFSA1CNT"}
{"MSGUOW1":"X15APPL D5B90B87EA823F90","MSGIDSTN":"ASDF    ","MSGODSTN":"PART    ","MSGXDATA_ALL":"PART WAY","MSGXDATA_ALL_LEN":"000
{"MSGUOW1":"X15APPL D5B90B87EA823F90","MSGIDSTN":"ASDF    ","MSGODSTN":"ASDF    ","MSGXDATA_ALL":"Part Number WAY not in Data Base"
{"MSGUOW1":"X15APPL D5B90B8865E38583","MSGIDSTN":"        ","MSGODSTN":"DFSA1CNT"}
{"MSGUOW1":"X15APPL D5B90B8D0635D581","MSGIDSTN":"        ","MSGODSTN":"SMASTER ","MSGXDATA_ALL":"\/DIS STATUS NODE C430     USER A
{"MSGUOW1":"X15APPL D5B90B8D063C2FA0","MSGIDSTN":"ASDF    ","MSGODSTN":"ASDF    ","MSGXDATA_ALL":".    **TRAN****PSBNAME.....    BM
{"MSGUOW1":"X15APPL D5B90B8D0635D581","MSGXDATA_ALL":"    IVPDB1    NOTOPEN NODE C430     USER ASDF    .....    IVPDB1I   NOTOPEN N
{"MSGUOW1":"X15APPL D5B90B8D063C2FA0","MSGXDATA_ALL":"    BMCTST02  NOTINIT.....    BMCTST03  NOTINIT.....    BMCTST04  NOTINIT....
{"MSGUOW1":"X15APPL D5B90B8D0635D581","MSGXDATA_ALL":"    FMQPSB    NOTINIT NODE C430     USER ASDF    .....    IOPBMP    NOTINIT N
{"MSGUOW1":"X15APPL D5B90B8D0635D581","MSGXDATA_ALL":"    -N\/A         DISCONNECTED NODE C430     USER ASDF    .....    -N\/A
{"MSGUOW1":"X15APPL D5B90B8D063C2FA0","MSGXDATA_ALL":"    -N\/A         DISCONNECTED.....    -N\/A         DISCONNECTED.....    -
{"MSGUOW1":"X15APPL D5B90B8D0635D581","MSGXDATA_ALL":"    -N\/A         DISCONNECTED NODE C430     USER ASDF    .....    -N\/A
{"MSGUOW1":"X15APPL D5B90B8D063C2FA0","MSGXDATA_ALL":"    -N\/A         DISCONNECTED.....    -N\/A         DISCONNECTED.....    -
{"MSGUOW1":"X15APPL D5B90B8D0635D581","MSGXDATA_ALL":"    -N\/A         DISCONNECTED NODE C430     USER ASDF    .....    -N\/A
```

BMC AMI Defender for IMS V.3.0.01 (New Features)



BMC AMI Defender for IMS (New Features)

Agenda

- New changes for the new BMC AMI Defender for Z/OS (CZAGENT) v6.0.02
- New Database Change Capture (F8 Log record type).
- New User Exit for extraction.
- New option in the ISPF AFI server for sending records to the CZAGENT

- BMC AMI Defender for IMS
- V3.0.01

New changes for the BMC AMI Defender for Z/OS (CZAGENT) v6.0.02

New changes for the CZAGENT v6.0.02

There are some changes that need to be consider to enable the IMS extraction in the BMC AMI Defender for ZOS V6.0.02

- This CZAGENT release provide the following members that used to be in our BMC AMI Defender for IMS .AFISAMP library:
  - CZAPARMS
  - CZDIMS
  - CZDUSER3
  - CZPIMS

New changes for the CZAGENT v6.0.02

Before when we install the BMC AMI Defender for Z/OS the following library was gotten:

- CZAGENT.CNTL to set the all parameters needed.

Now when we install the BMC AMI Defender for Z/OS V6.0.02 the following libraries are gotten:

- CZAGENT.CNTL it has sample members for CZAGENT
- CZAGENT.PARM to set the all parameters needed.

New changes for the CZAGENT v6.0.02

- There are some options than needs to be enabled in the following CZAGENT PARM members for the IMS extraction:
  - Select (uncomment) the IMS SWITCH option in the member **CZAGENT.PARM($$$CONFG)** as follow:

    SWITCH ON(IMSLOG) ; IMS Log Record Events

- The SELECT EVENTs for the IMS are now included in the CZAGENT.PARM($$$SELCT) for BMC Defender for zOS (CZAGENT) v6.0.02 package.

- BMC AMI Defender for IMS
- V3.0.01

New Database Change Capture (F8 Log record type).

New Database Change Capture (F8 LR)

- For this release a new log record type is added, the new F8 log record type is used for BMC AMI Defender for IMS to get the IMS Database Capture information registering the DB calls such as Inserts, Updates or Deletes and also they can be filtered by DB name or User ID.

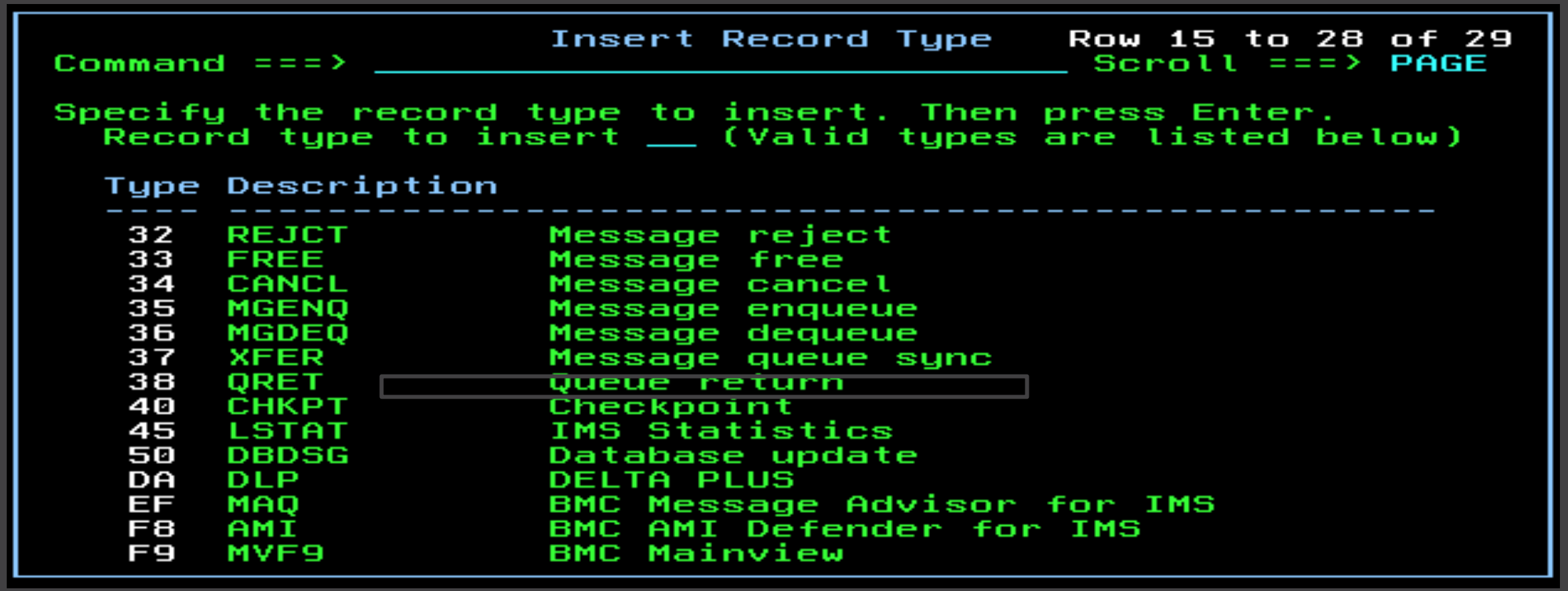
- The new F8 log record provides fields with relevant data like Subcodes to refer a Database Updates (03) including Key and Concatenated key data, Application Start (04) and Application Terminate (05).

- This F8 log record is registered in the IMS logs with the extracted data based on the user criteria

New Database Change Capture (F8 LR)

- The new F8 log record can be chosen in the Extract list member and in the CZAINTXI member.

Extract list selection



New Database Change Capture (F8 LR)

CZAINTXI for CZAGENT

```
VIEW        DCE.CQVF1.VF1P.PROCLIB(CZAINTXI) - 01.59          Columns 00001 0007
Command ===>                                                  Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001 *-------------------------------------------------------------------*
000002 * IMS Initialization exit INPUT PARMS                               *
000003 *                                                                   *
000004 * Name:     CZAINTXI                                                *
000005 *                                                                   *
000006 * Purpose: Config member for BMC IMS Log Writer Exit.               *
000007 *          - Define Log type records to pass to CZA Agent.          *
000008 *          - Parm values are passed in the IMS Exit User area.      *
000009 *                                                                   *
000010 * (c) Copyright 2015-2019 BMC Software, Inc.                        *
000011 *-------------------------------------------------------------------*
000012 TRACE=0                        - Write Traces 1-5
000013 IMSID=VF1P                     - IMS Subsystem ID
000014 CALLZDEFENDER=Y                - Y|N to pass Records to zDefender
000015 ZDEFENDER=ALEX.CCT.Agent       - Default Instance name char(16)
000016 MAXLEN=1010                    - nnnn max len of Type 01/03 rec -> API
000017 *-------------------------------------------------------------------*
000018 * The LOGTYPEs below are currently supported. Edit as required.
000019 * Scroll to bottom to see detailed explanation of Parms and syntax.
000020 *-------------------------------------------------------------------*
000021 *LOGTYPE=ALL
000022 *LOGTYPE=01
000023 *LOGTYPE=03
000024 *LOGTYPE=10
000025 *LOGTYPE=16
000026 *LOGTYPE=22
000027 *LOGTYPE=24
000028 *LOGTYPE=50
000029 LOGTYPE=F8
000030
```

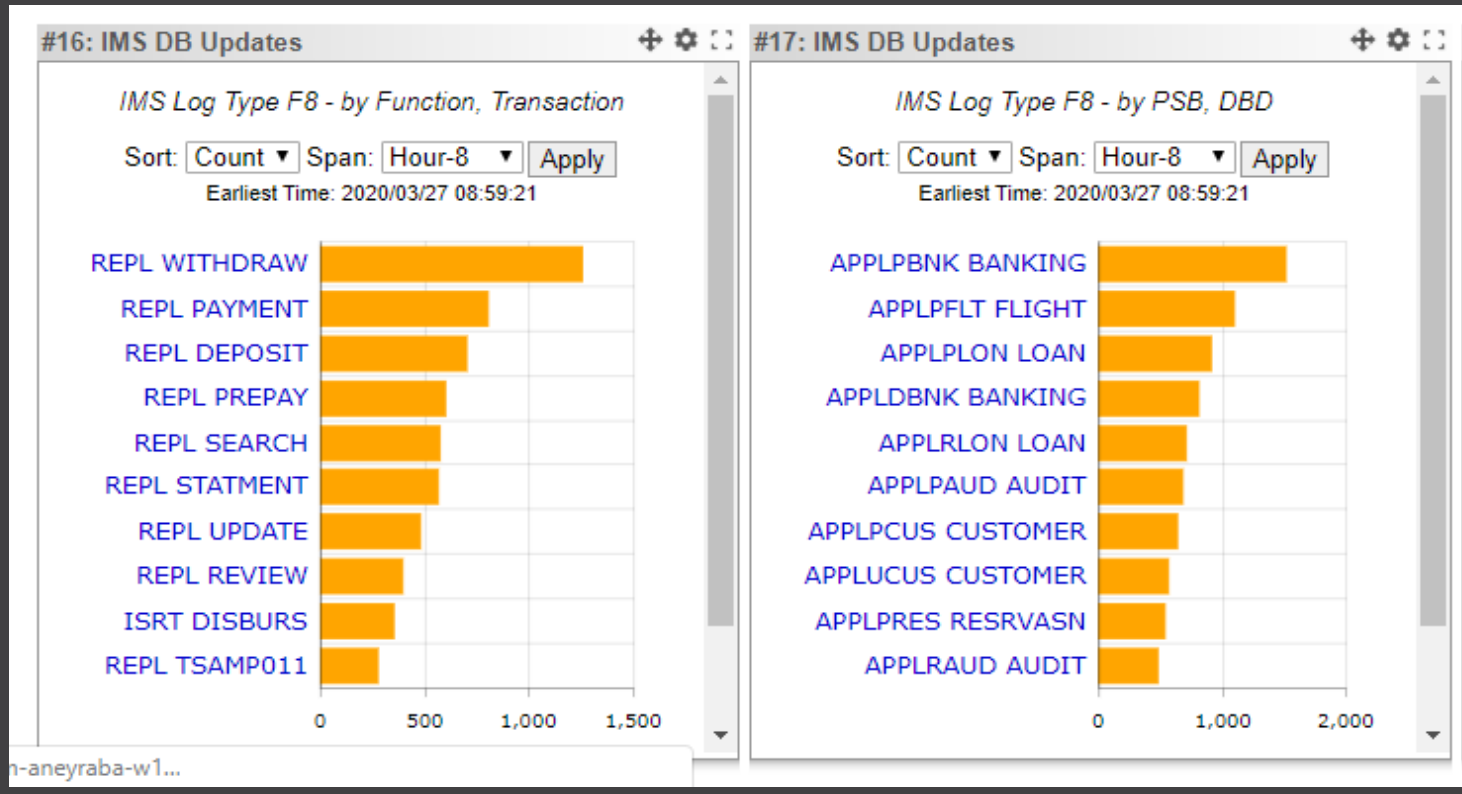
New Database Change Capture (F8 LR)

- A new DD is added for enabling the new F8 log record creation in the BMC AMI Defender for IMS PROC; The //DBFILTER DD sample member contains the DB calls/DB name/USERID criteria to generate the F8 log records.

```
 File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
VIEW        DCE.CQVF1.VF1P.PROCLIB(DBFILTER) - 01.03          Columns 00001 00072
Command ===>                                                  Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001 *-------------------------------------------
000002 *
000003 *     DB FILTER DATASET
000004 *     DBCALL=ISRT/REPL/DLET
000005 *            CHOOSE WHAT FUNCTION CALL TO CAPTURE. AT LEAST 1 IS REQUIRED
000006 *            TO CAPTURE UPDATES.
000007 *     DBNAME=DATA
000008 *            DATABASE NAME TO CAPTURE. MAY USE '*' AND '?' MATCHING CHARS
000009 *     USERID=DATA
000010 *            USERID TO CAPTURE. MAY USE '*' AND '?' MATCHING CHARS.
000011 *
000012 *     IF DBNAME IS NOT SPECIFIED ALL DB'S WILL BE CAPTURED.
000013 *     IF USERID IS NOT SPECIFIED ALL USERS WILL BE CAPTURED.
000014 *
000015 *     WILDCARD CHARACTERS '*' AND '?'
000016 *            '?' CAN BE USED ANYWHERE IN THE STRING, AND WILL MATCH ANY
000017 *                1 CHARACTER. E.G. IV??B2 WILL MATCH IVPDB2 AND IVXXB2 BU
000018 *                NOT IVB2.
000019 *            '*' CAN BE USED AT THE END OF A STRING TO MATCH 0 OR MORE
000020 *                CHARS. E.G. IVP* WILL MATCH IVP, IVPDB2 OR IVPD, BUT NOT
000021 *                IVC.
000022 *-------------------------------------------
000023 DBCALL=ISRT
000024 DBCALL=REPL
000025 DBCALL=DLET
000026 *DBNAME=IV??B?
000027 *USERID=MVSAQN8C
****** ***************************** Bottom of Data ***************************
```

New Database Change Capture (F8 LR)

- Also, to enable the F8 log record in the IMS the BMD DLI library must be concatenated in the IMS CNTL, DBRC and DLI regions.
- New IMS Dashboards for the new F8 log records are added in the Command Center Version 6.0.02 Build 3061.



- BMC AMI Defender for IMS
- V3.0.01

New user exit for extraction

New user exit for extraction

- This BMC AMI Defender for IMS release provides an user exit to enable the extraction as well, the sample user exit is located in the AFISAMP install library and the load module has to be in STEPLIB in BMC AMI Defender for IMS PROC; another DD is required in the PROC for the user exit which is //UEXITOUT DD to get the extracted data in this data set.

New user exit for extraction

User exit load module in STEPLIB

//UEXITOUT DD to get the extracted data

```
 File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
VIEW        SYS3.PROD.PROCLIB(AQNAFI15) - 01.99              Columns 00001 00072
Command ===>                                                 Scroll ===> CSR
****** ******************************** Top of Data ********************************
000001 //AQNAFI15  PROC
000002 //*
000003 //*       APF AUTHORIZE THE DATASETS IN XRBA STEPLIB
000004 //*
000005 //JTHAPF00  EXEC  PGM=JTHAPF00,ACCT=(5920),REGION=0M,
000006 //         PARM='AFI00,STEPLIB'
000007 //*
000008 //AFI00     EXEC PGM=AFICTL00,REGION=500M,DYNAMNBR=99,
000009 //          ACCT=(5510),PARM='A5AF'   * CHANGE @@@@ TO YOUR 4-CHAR ID
000010 //*
000011 //STEPLIB  DD DISP=SHR,DSN=IMSB.ICO.XTSTA.ICOLIB
000012 //* -------------- TESTING AFI V3.0.00  -------------------------*
000013 //*
000014 //          DD DISP=SHR,DSN=MVSAQN1.AFIV300.OPTIONS
000015 //          DD DISP=SHR,DSN=AFI.V30.LOAD
000016 //          DD DISP=SHR,DSN=MVSSNN.AFI30.UEXIT.CASE001.LOAD
000017 //          DD DISP=SHR,DSN=IMSB.ALL.ITSTA.XXLINK
000018 //*
000019 //DBFILTER DD DISP=SHR,DSN=DCE.CQVF1.VF1P.PROCLIB(DBFILTER)
000020 //*
000021 //*+++++++++++++++++  AFI USER EXIT  ++++++++++++++++++++++++++++++ *
000022 //UEXITOUT DD DSN=MVSAQN1.AFIV300.AFIUEXIT.OUT15,DISP=SHR
000023 //*           SPACE=(CYL,(10,5)),
000024 //*           DISP=(NEW,CATLG,CATLG),
000025 //*           DCB=(LRECL=32756,BLKSIZE=0,RECFM=FB)
000026 //*
000027 //* ------------------------------------------------------------*
000028 //BMCPSWD  DD DISP=SHR,DSN=SLJ.PSWD.PERM
000029 //***------ BMC AMI DEFENDER  FOR IMS ----------------
000030 //SYSIN    DD DISP=SHR,DSN=DCE.CQVF1.VF1P.PROCLIB(CZAINTXI)
000031 //CZAILOGD DD DISP=SHR,DSN=DCE.CQVF1.VF1P.PROCLIB(CZAILOGD)
```

New user exit for extraction

When the USER EXIT is enabled the following messages will be received in the AFI server log:

```
BMCAFI001012I User exit routine AFIUEXIT loaded
AFIUEXIT Init start                          It indicates that the User
AFIUEXIT Init complete                       exit was initialized.
AFIUEXIT send start                          it is displayed every time
AFIUEXIT send complete                       that a log records is extracted
AFIUEXIT Term start                          it is displayed when the user exist is
AFIUEXIT Term complete                       terminated because the AFI server is
stopped
```

- BMC AMI Defender for IMS
- V3.0.01

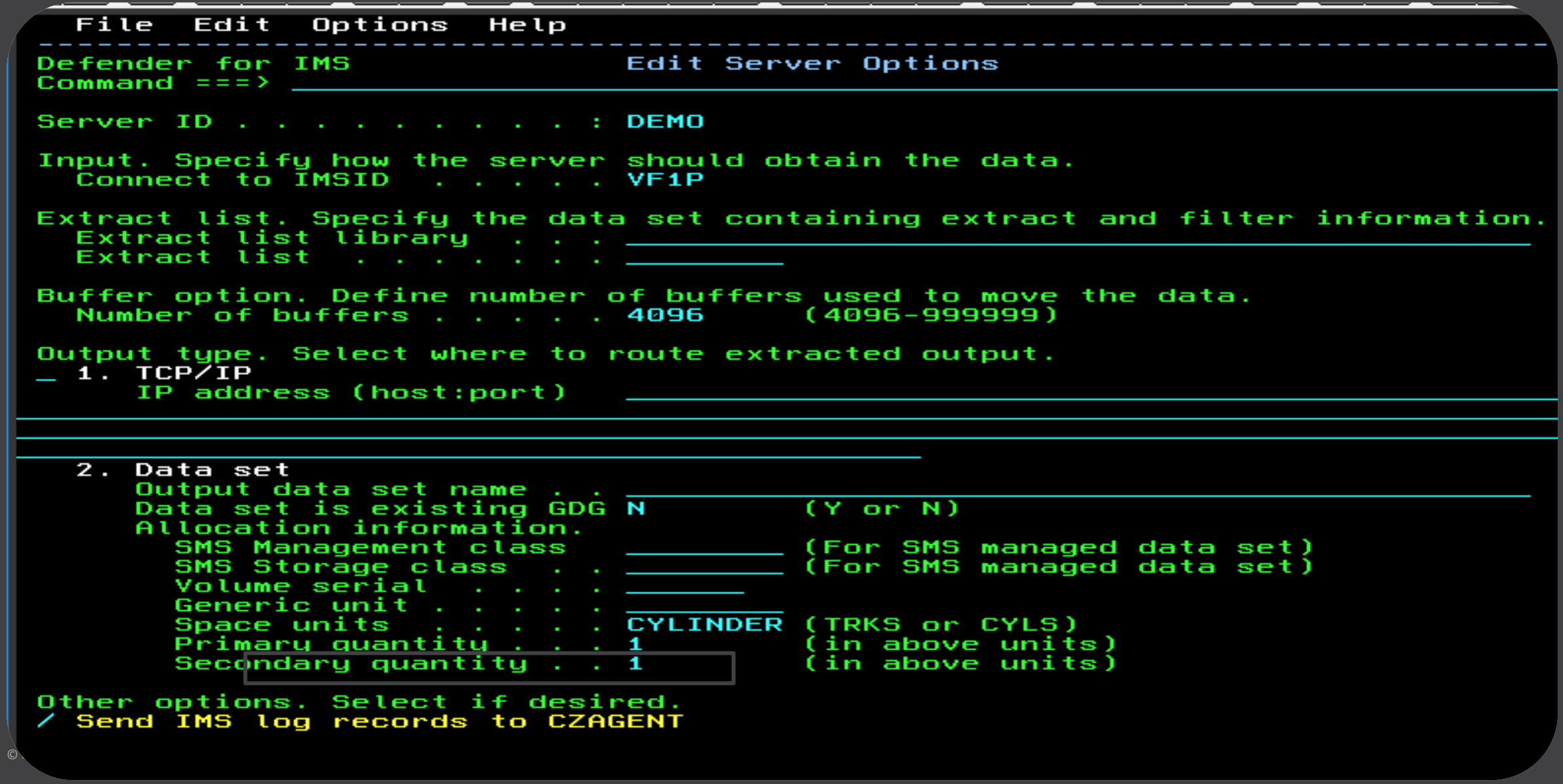
New option in the ISPF AFI server for sending records to the CZAGENT

New option in the ISPF AFI server for CZAGENT

- A new option was added to the ISPF Server options to enable or disable sending IMS log records to the CZAGENT (BMC Defender subsystem). The log record types to be sent are specified in the SYSIN DD of the BMC AMI Defender for IMS server.

- This option allows to customer decides if they want to send log records only through the CZAGENT without using Extract list member. If so the only requisite here is to set the IMSID, mark the option ‘Send IMS log records to CZAGENT’ and make sure that the //SYSIN and //CZAILOGD DDs are set in the AFI Server PROC.

New option in the ISPF AFI server for CZAGENT



What you need to do.

Truth

- Mainframes are more connected, so they are more susceptible to security attacks.
- It's easy to miss the breaches in the expansive capacity and speed of the mainframe. Event logs may be massive. Data fields are overwhelming.
- The mainframe can be hacked. IMS data can be compromised.

Action

- Use efficient tools and facilities to capture the right data in a timely manner.
- Take the potential threats seriously.
- Protect your business with intelligent analytics that detect events and patterns that could affect you.

Thanks!