GSE | GUIDE SHARE EUROPE

UK Region

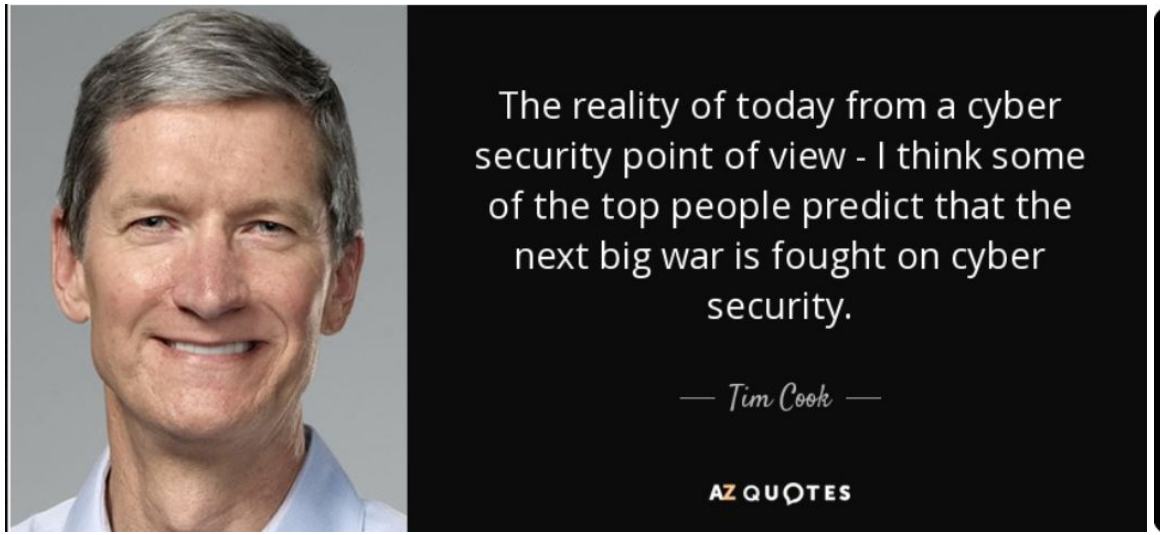
GSE UK VIRTUAL CONFERENCE 2024

Deal with growing cybersecurity risks and do Real-time and after-the-event IMS analytics, all at the same time

Santosh Belgaonkar
Sahil Gupta
BMC Software

April 2024
Session 2D

What is Cybersecurity?


The reality of today from a cyber security point of view - I think some of the top people predict that the next big war is fought on cyber security.
— Tim Cook —
AZ QUOTES


"There are only two types of companies:
those that have been hacked,
and those that will be."
Robert Mueller
FBI Director, 2012

Mainframes get it done!

- 71 Percent of Fortune 500 Companies Use Mainframes.
- Mainframes handle 90 percent of all credit card transactions.
- Mainframes handle 1 trillion business transactions each day.
- 60% of data available on internet is stored on mainframes.
- Mainframes handle 68% of world's production IT workloads

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?

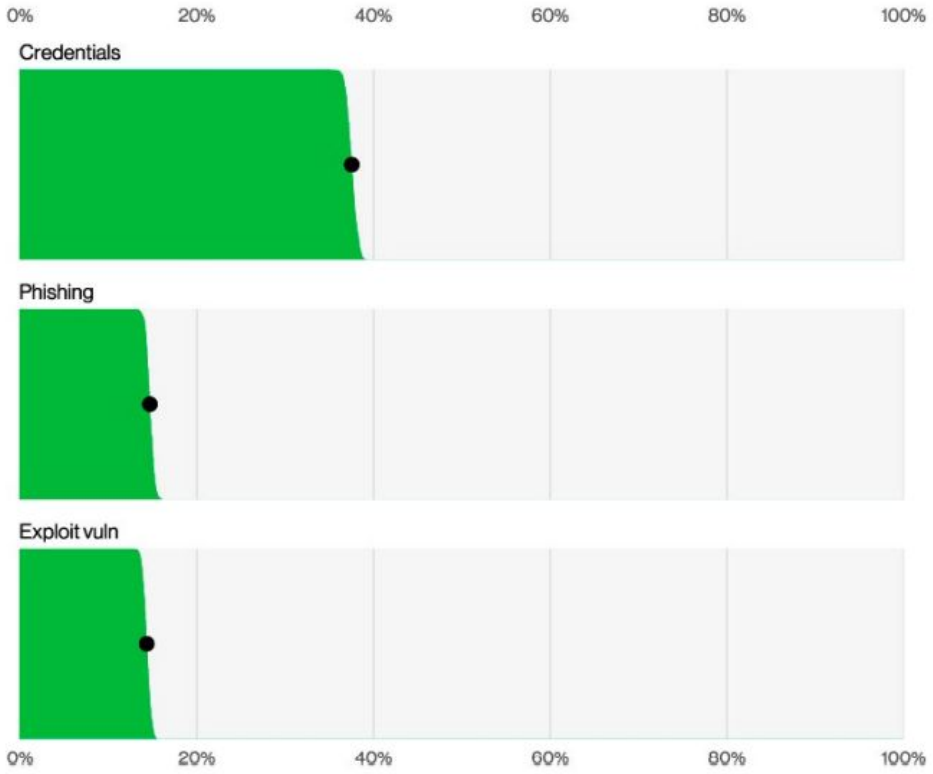
The Mainframe Can Be Hacked

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.

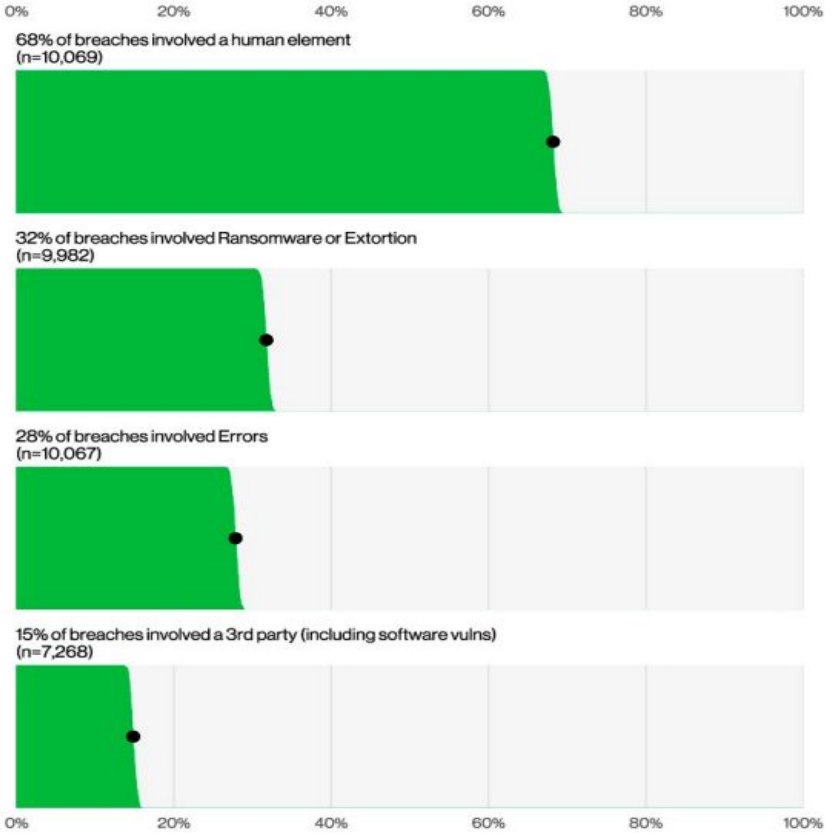
2012 – Co-founder of Pirate Bay and prominent hacker, Gottfrid Svartholm Warg, hacked into the CSC mainframe and stole hundreds of thousands of Danish social security numbers along with other important personal information stored in the mainframe.

2008 – Luxottica, 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

2024 Data breach investigations report



Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.



2024 Breaches by the Numbers

194 Days — Mean time to identify breach

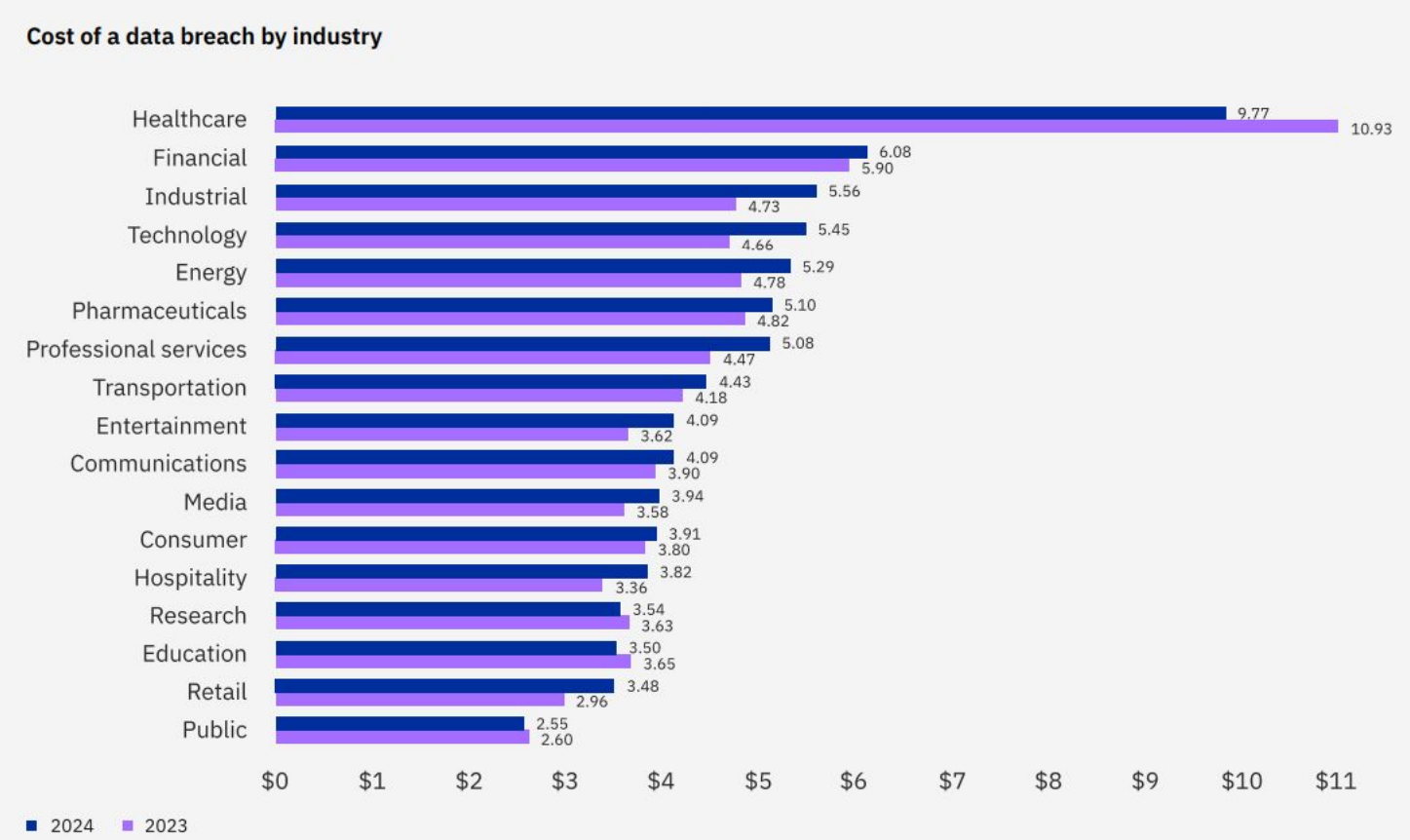
$4.88 M — Global average cost of data breach

70% — Share of organizations that experienced a significant or very significant disruption to business because of a breach

$4.99 M — Average cost of a malicious insider attack

$9.36 M — Average total cost of data breach in US

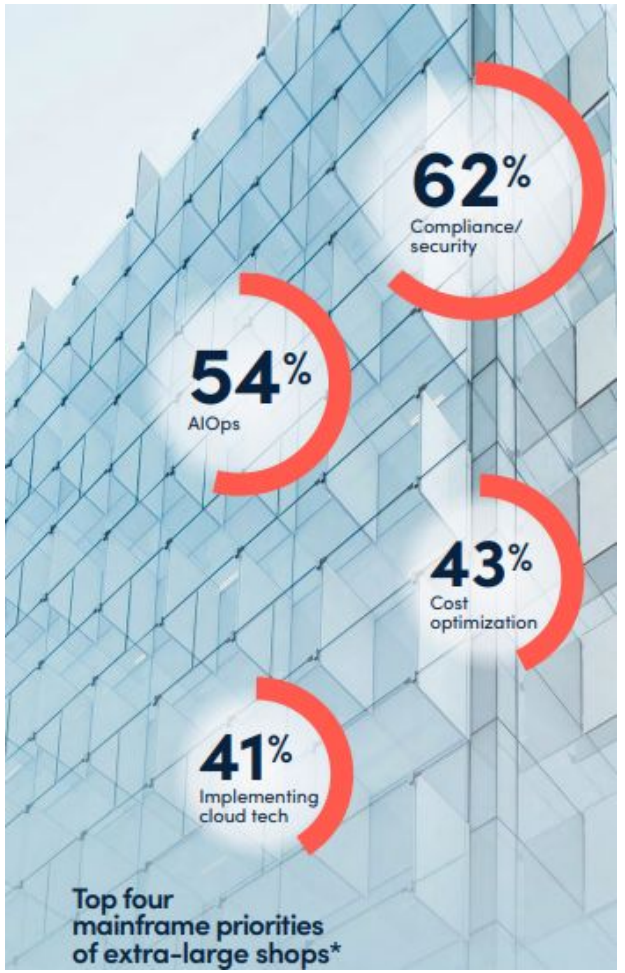
2024 Breaches by the Numbers (Continued…)



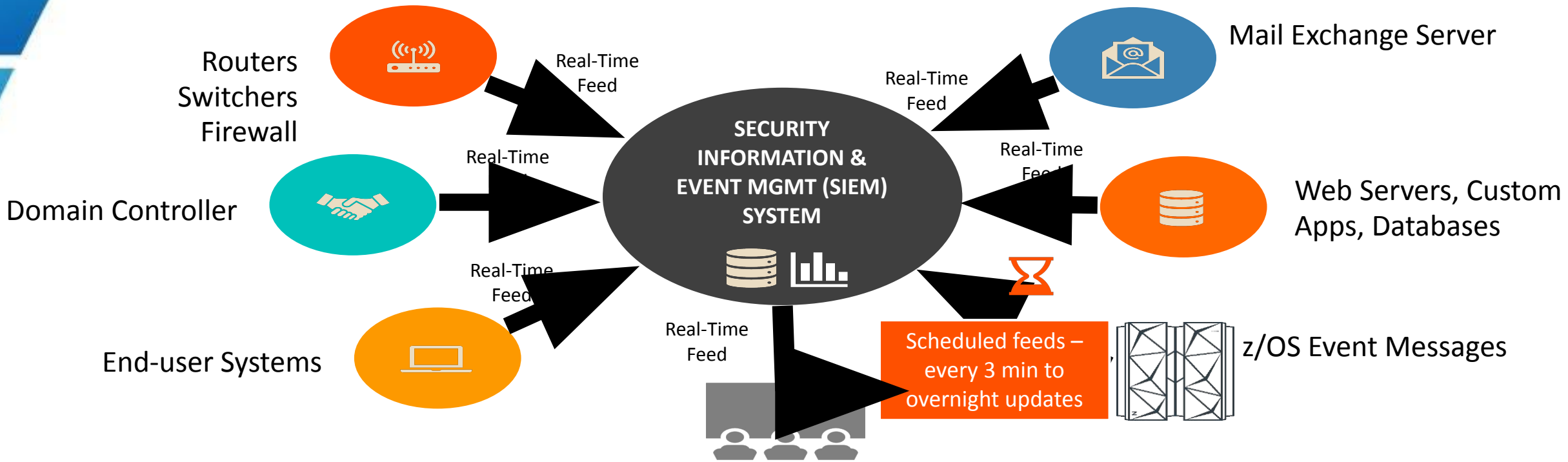
BMCs 2024 mainframe survey says…

- Compliance and security are the top priority for survey respondents for the fifth year in a row, named by 62% of respondents.

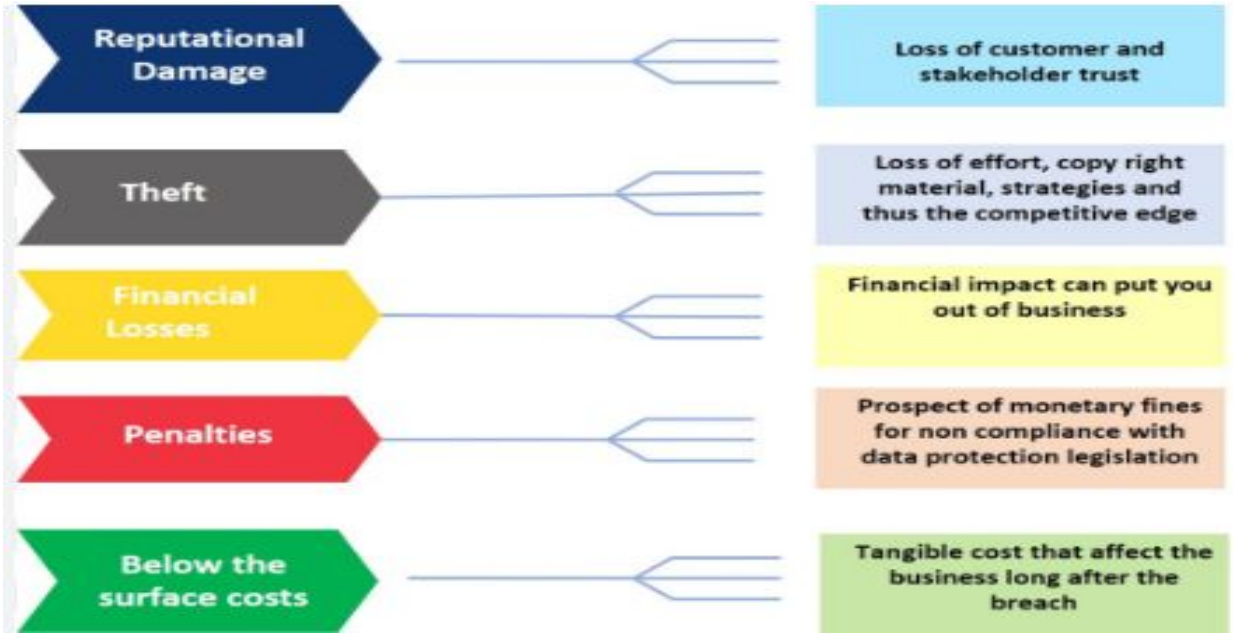
- 43% have built dedicated capabilities to protect against ransomware and 29% plan to build capabilities.



SIEM Feeds the SOC with Real-time Security Events, but the Mainframe…

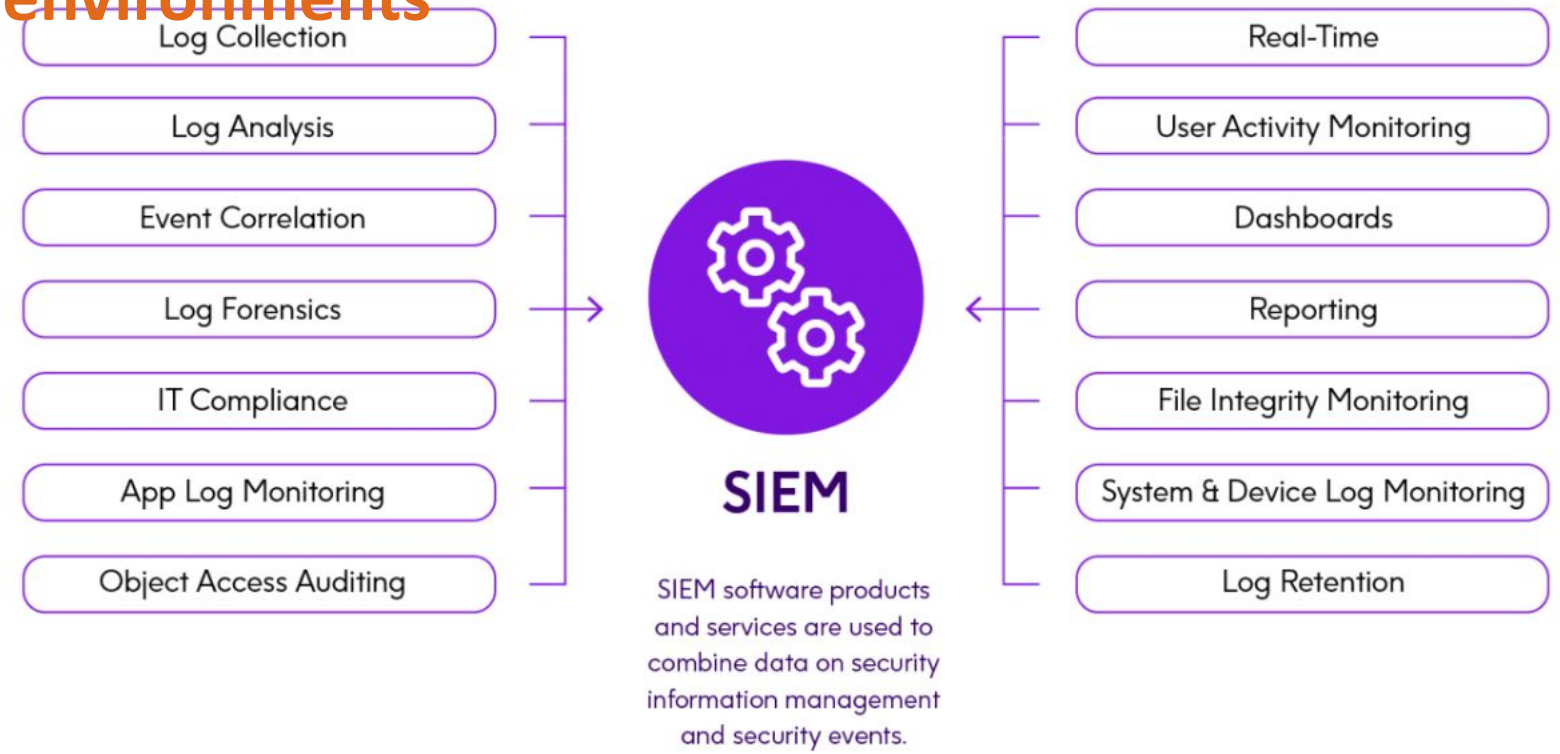


Consequences of cybersecurity breaches



Sources of Cybersecurity threats

Key aspects of cybersecurity in mainframe environments



The world depends upon IMS

IMS processes **the world's** transactions

50,000,000,000
(50 billion) secure transactions per day

What would you do with 100,000 transactions per second?

IMS is not just keeping pace with the industry, it is leading the way in performance. In 2013 IBM announced that the current version of IMS reached a revolutionary benchmark of 117,292 transactions per second. **Nothing else comes close.**

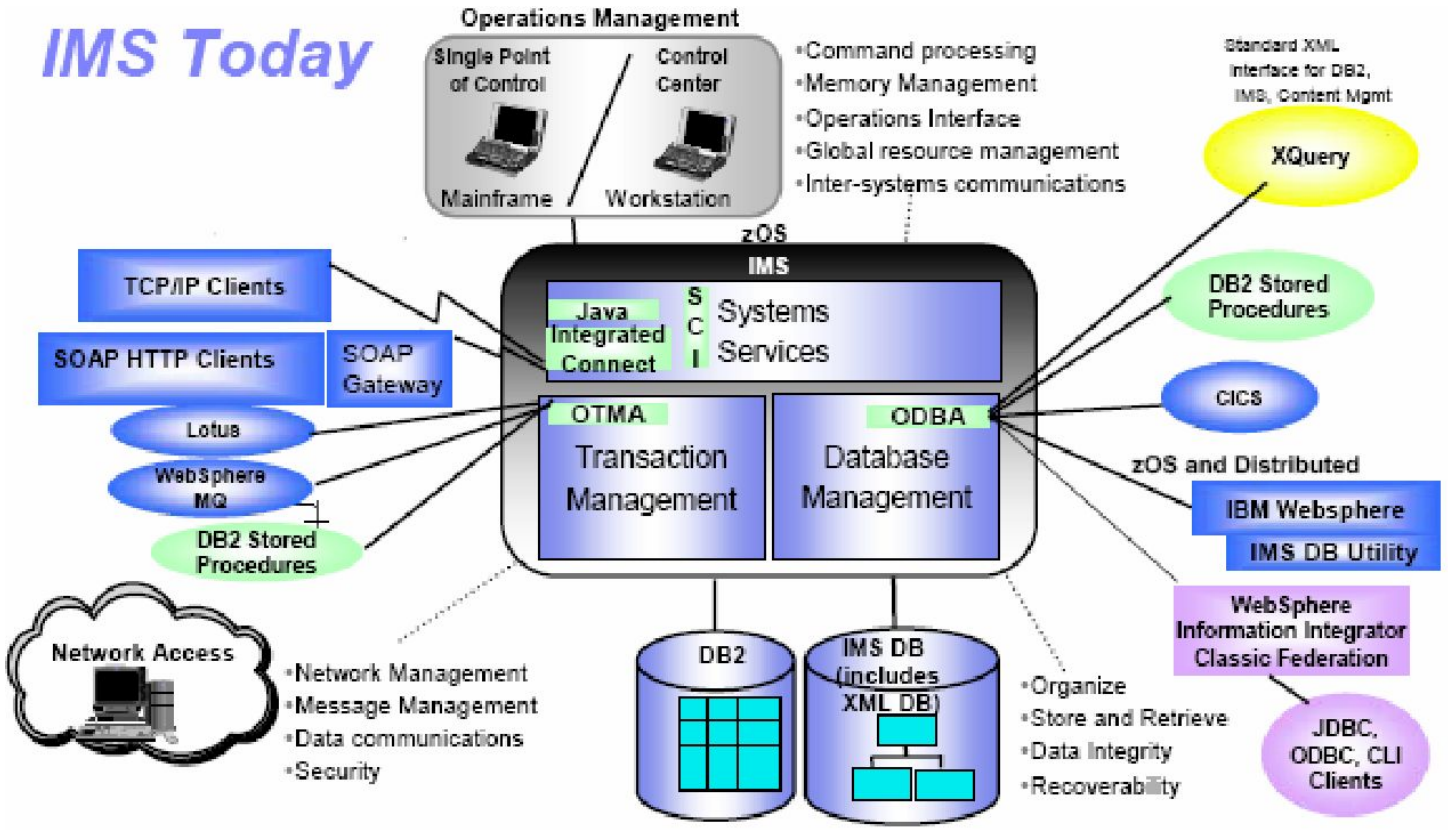
This translates to 528 transactions per year for every single person on the planet. And it's not throwaway data like tweets or posts. It's your most critical data, safe, secure, available.

117,292
transactions per second

Businesses worldwide have come to understand that sooner than later, they will see workloads that inch closer and closer to these speeds and volumes. **IMS is ready.** Are you?

Not just terminals accessing IMS

IMS is more connected than ever

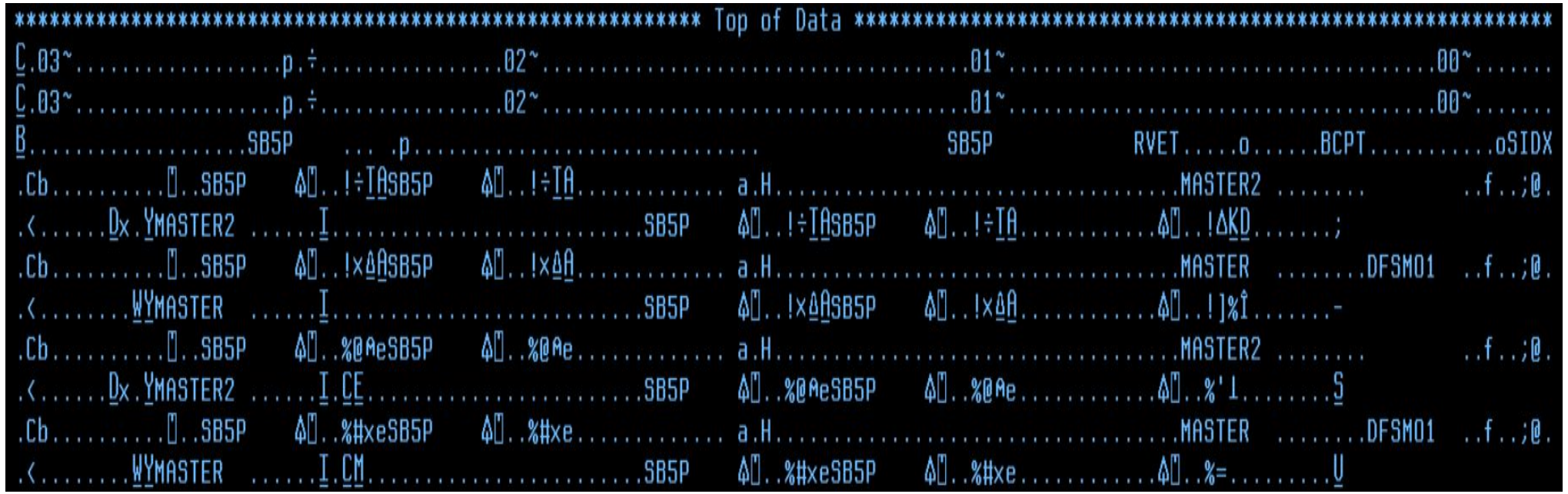


Real-time monitoring

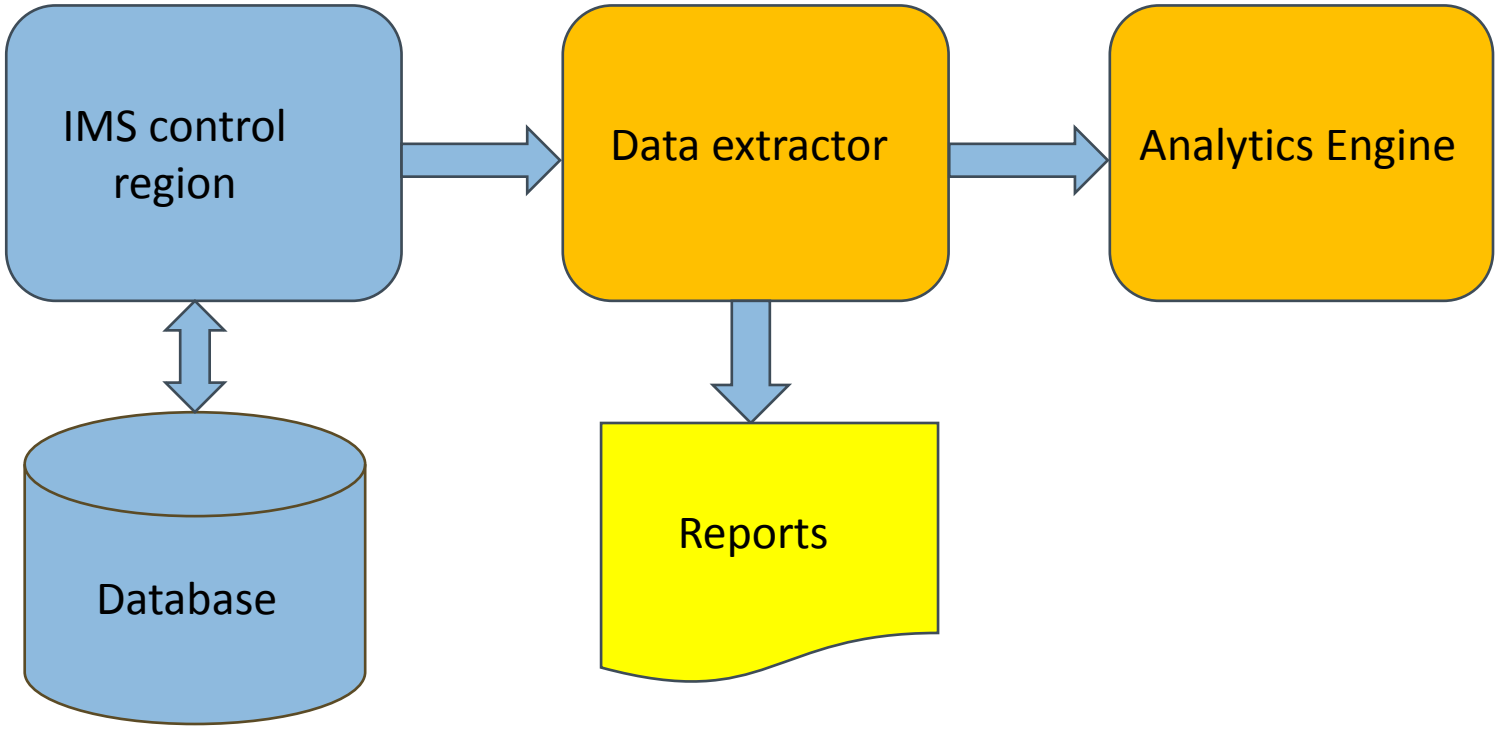
"Near real time" is not good enough!

IMS logs are massive…

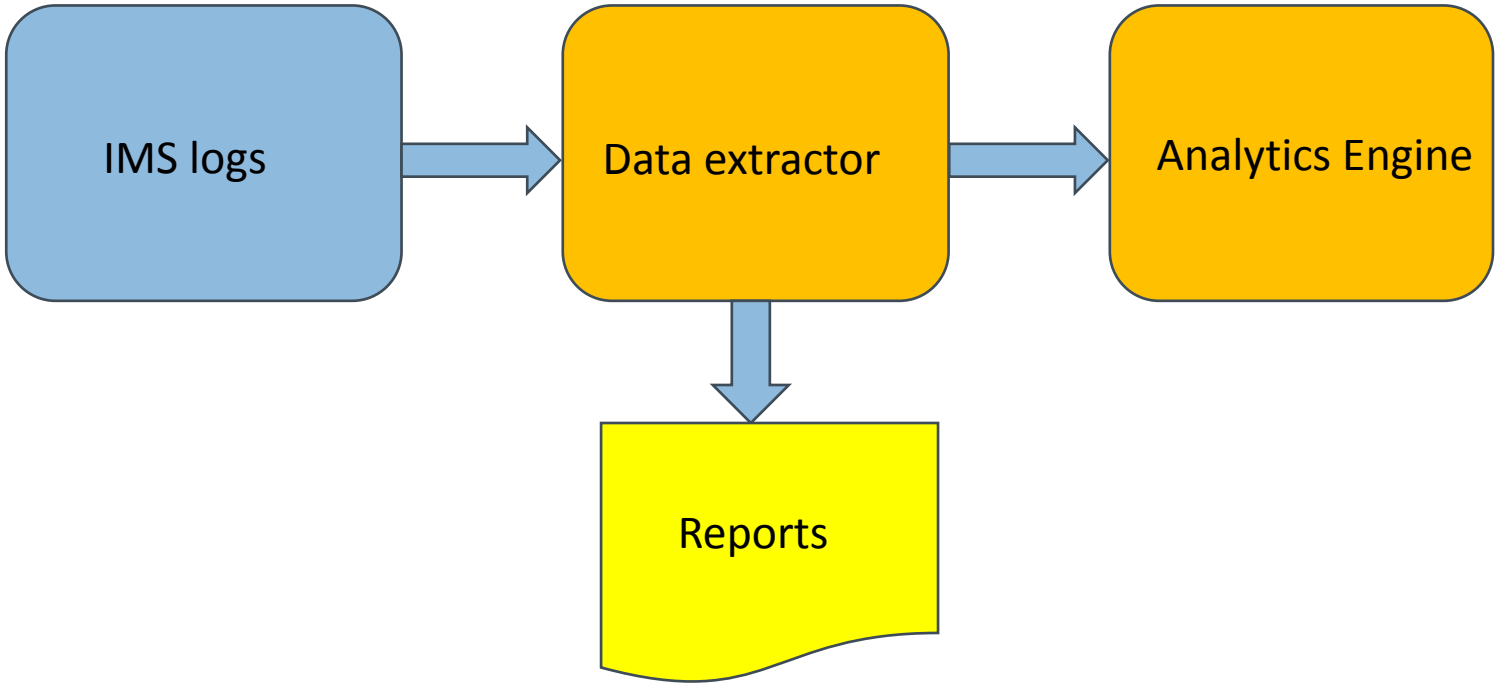
IMS logs are difficult to read and comprehend in their native raw format



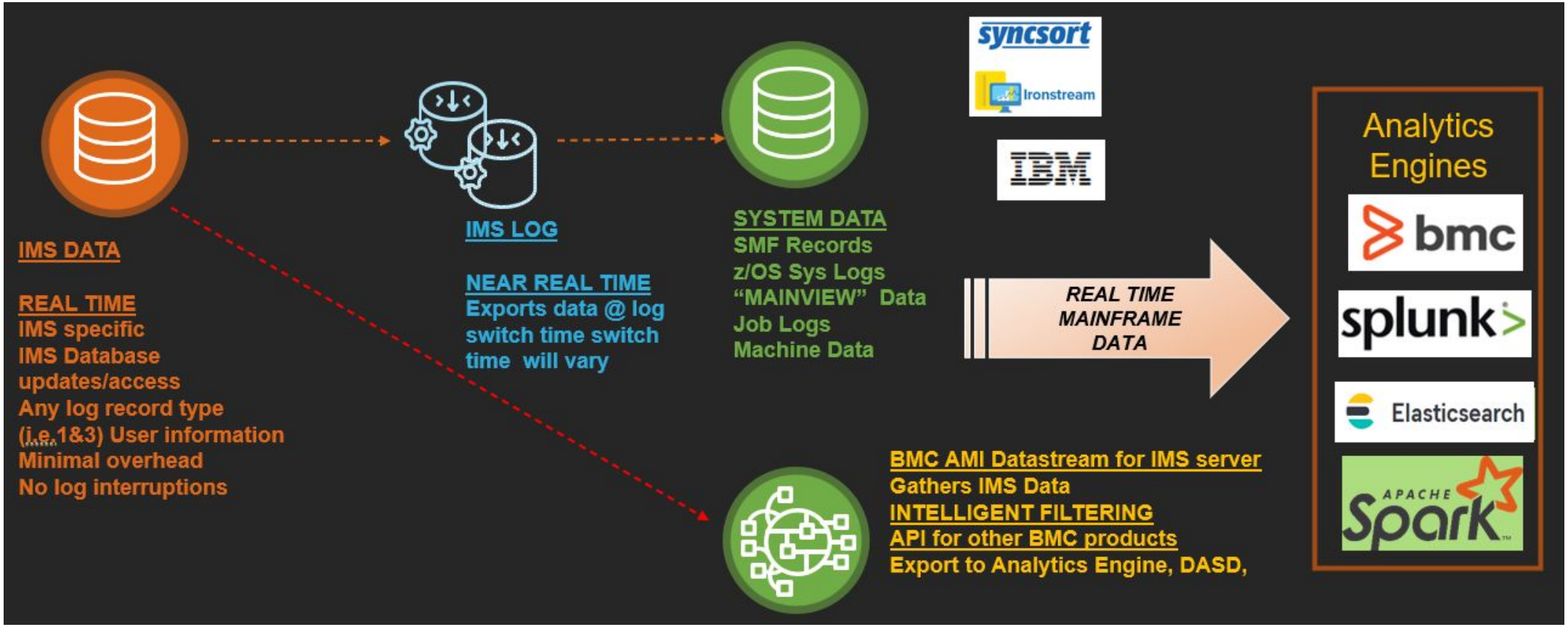
Real-time processing



After-the-event processing



Mainframe Data Extraction Providers



Log record X'10' - Security Violation record

A	Field Name	Description	Type	Length
_	IMSID	IMS ID	STRING	4
_	LOGRC_LENGTH	Log record length	INTEGER	5
_	LOGRC_TYPE	Log record type	HEX	2
_	LOGRC_STCK	Log record timestamp	TIMESTMP	19
_	LOGRC_SEQUENCE_NUMBER	Log record sequence number	HEX	16
_	SCBTAMT	BTAM terminal violation	Y/N	1
_	SCVTAMT	VTAM terminal violation	Y/N	1
_	SCAOI	Application program violation	Y/N	1
_	SCERROR	Error code	INTEGER	5
_	SCERROR_TEXT	Error text	STRING	80
_	SCCMD	/+Command verb	STRING	4
_	SCLINE	Relative line number of violator	INTEGER	10
_	SCTERM	Relative terminal number of violator	INTEGER	10
_	SCNODE	VTAM node name	NAME	8
_	SCTRAN	Transaction code or userid	NAME	8
_	SCDST	Timestamp of violation	TIMESTMP	19
_	SCPGM	Program name (ICMD failure)	NAME	8

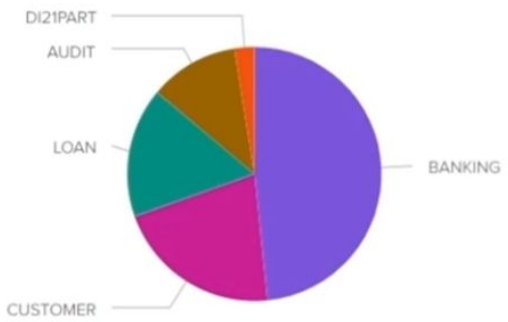
Log record X'16' – Sign on/Signoff record.

A	Field Name	Description	Type	Length
_	IMSID	IMS ID	STRING	4
_	LOGRC_LENGTH	Log record length	INTEGER	5
_	LOGRC_TYPE	Log record type	HEX	2
_	LOGRC_STCK	Log record timestamp	TIMESTMP	19
_	LOGRC_SEQUENCE_NUMBER	Log record sequence number	HEX	16
_	SGNTCPIP	Terminal is TCPIP	Y/N	1
_	SGNVTAM	Terminal is VTAM	Y/N	1
_	SGNBTAM	Terminal is BTAM	Y/N	1
_	SGNISCAL	Static ISC w/o signon	Y/N	1
_	SGNOFFRC	/Signoff forced	Y/N	1
_	SGNOFF	/Signoff	Y/N	1
_	SGNON	/Signon	Y/N	1
_	SGNASOFF	User was auto signed off	Y/N	1
_	SGNALLOC	User alloc/dealloc done	Y/N	1
_	SGNONSEC	Security bypass signon	Y/N	1
_	SGNNRNR	Session starts with NRNR	Y/N	1
_	SGNARNR	Session starts with ARNR	Y/N	1
_	SGNPCKN	User signon with PASSCHK=NO	Y/N	1
_	SGNONODE	Signed on using node descriptor	Y/N	1
_	SGNUSER	Userid	NAME	8
_	SGNTERM	Line and PTERM or node name	NAME	8
_	SGNGRPNM	SAF group name	NAME	8
_	SGNSPQNM	User structure name	NAME	8

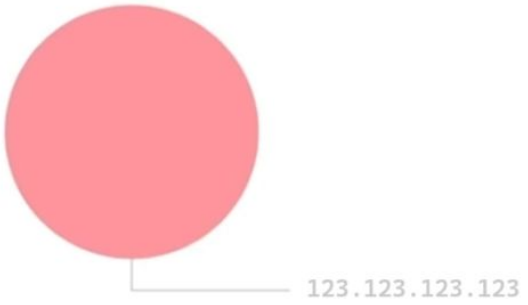
Monitor Sensitive Database READ log records

Database Read Stats

Top 10 - Database Reads

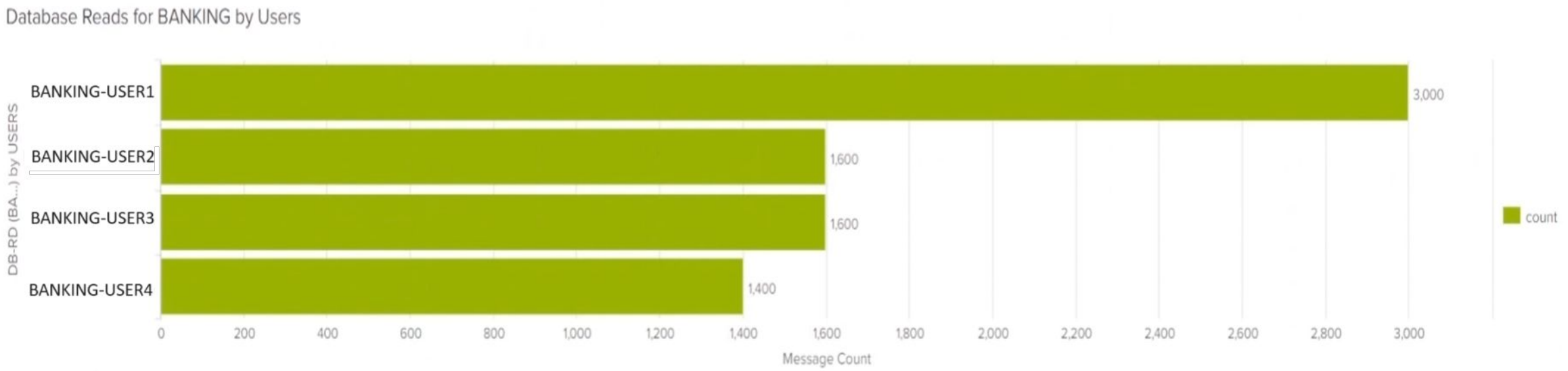


DB reads by LPAR



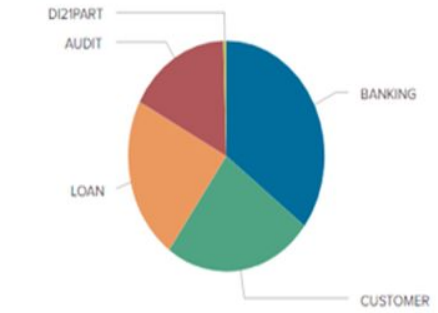
Database Reads by Users

Monitor sensitive database read activity by user

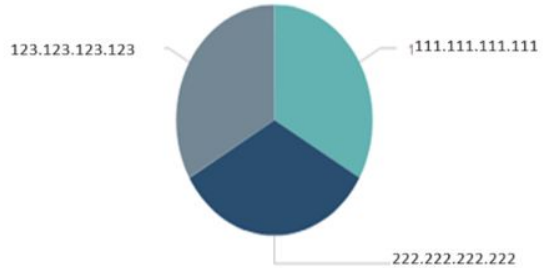


Database Update Stats

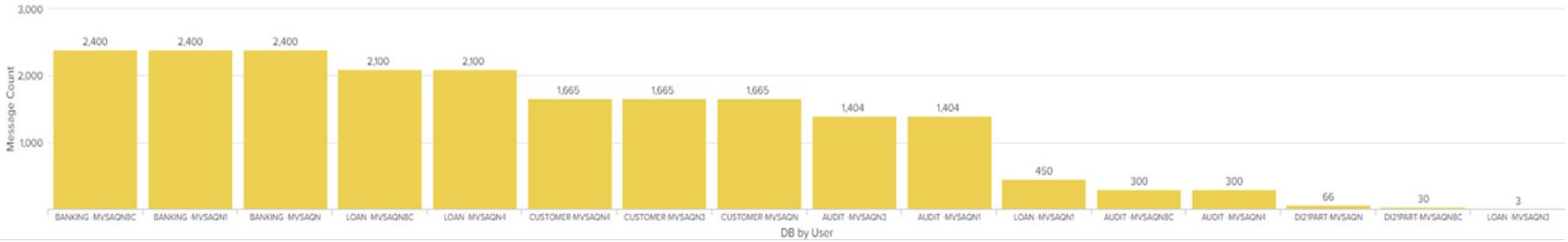
Database Updates - Top DBs



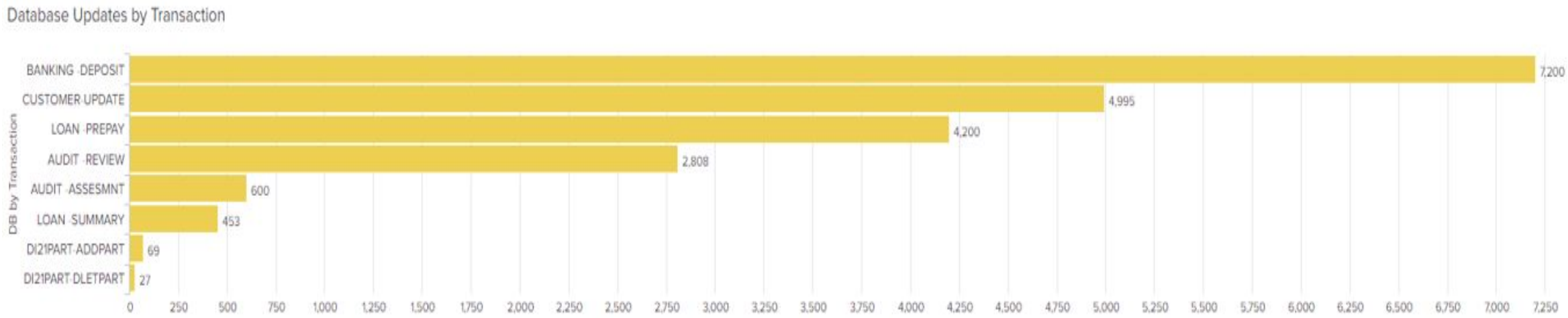
Database Updates by LPAR (IP address)



Database Updates by User



Database Update Stats (continued…)

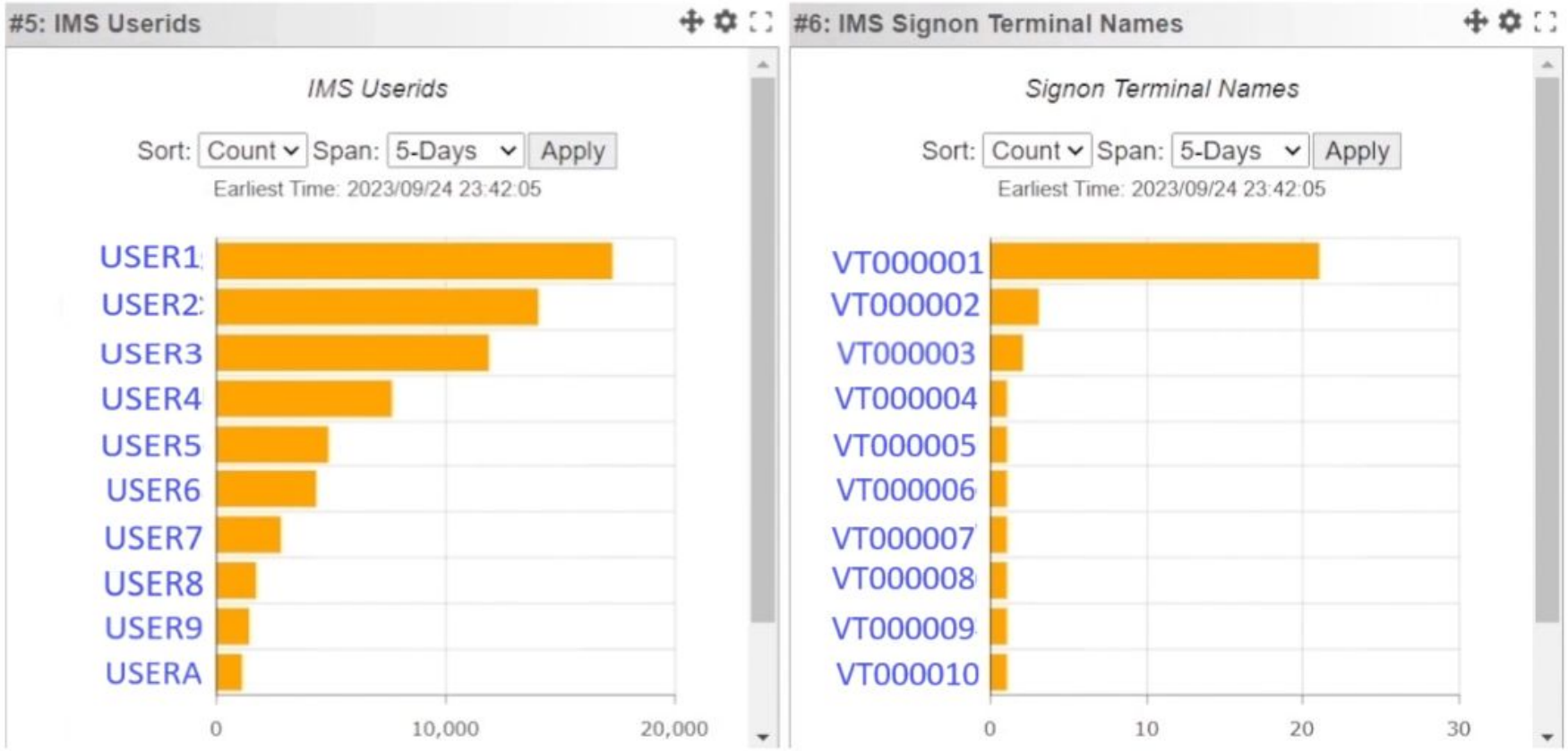


Security Violations

Security Violations (continued…)

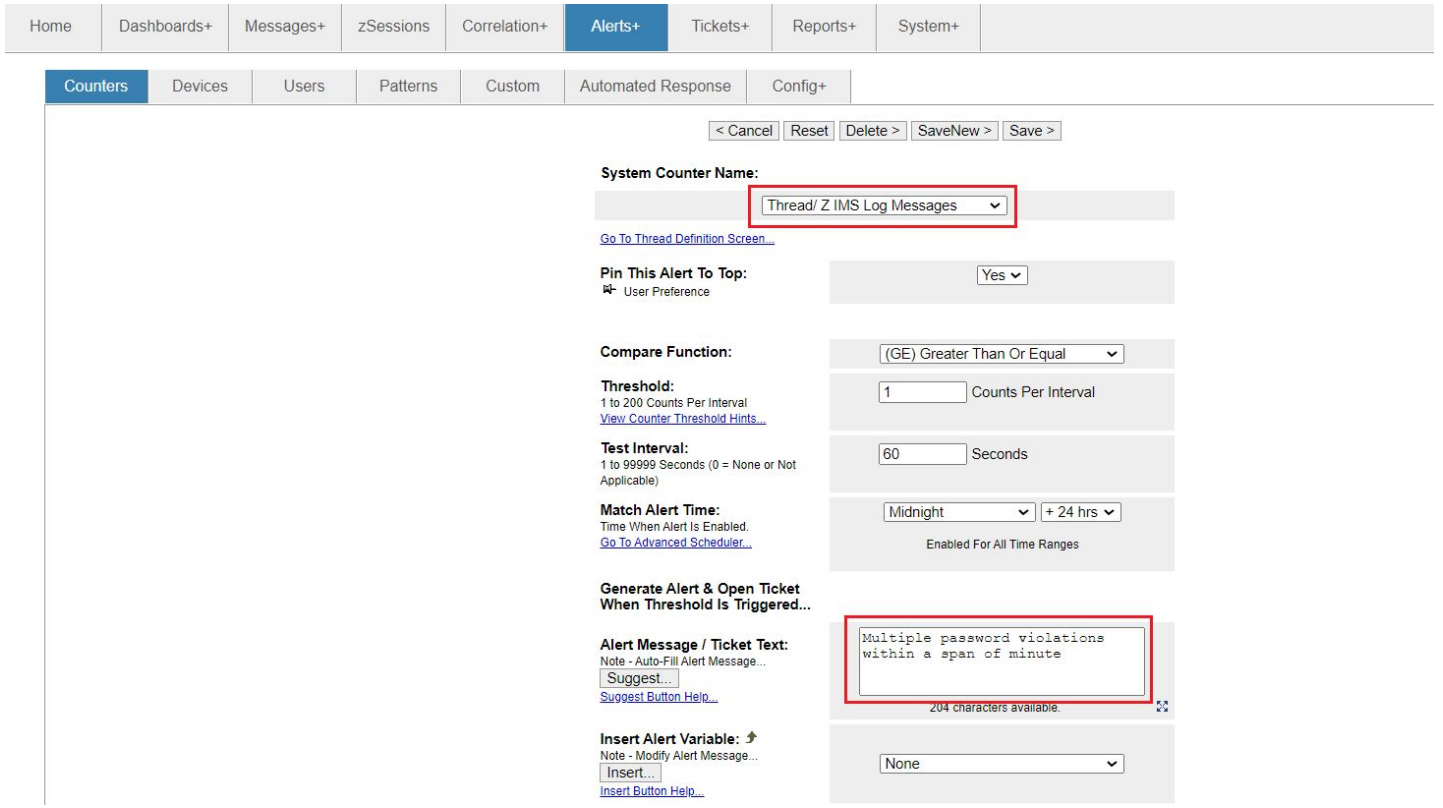
From IP Address:	123.123.123.123 xxx.xxx.com
Message Time:	2023/09/26 22:58:33 20 min, 7 sec ago
Message Facility:	audit
Message Severity:	info
Message Content:	Sep 27 05:58:35 SYSM IMS_10: SAF: 1 - SAFD: RACF - IMSID: VF1P - LogType: 10 - LogDesc: IMS Security Violation - FlagByte1: VTAM Terminal Violation - TypeOfError: PASSWORD NOT DEFINED OR USER NOT AUTHORIZED - CMDVerb: VTHB - RelLineNum: 3.86G - TermNum: 4.04G - VTAMNode: VTHB0551 - TranCode: MVSSYB - devTime: 2023-09-27T04:47:33.580

IMS user id and sign on terminal statistics

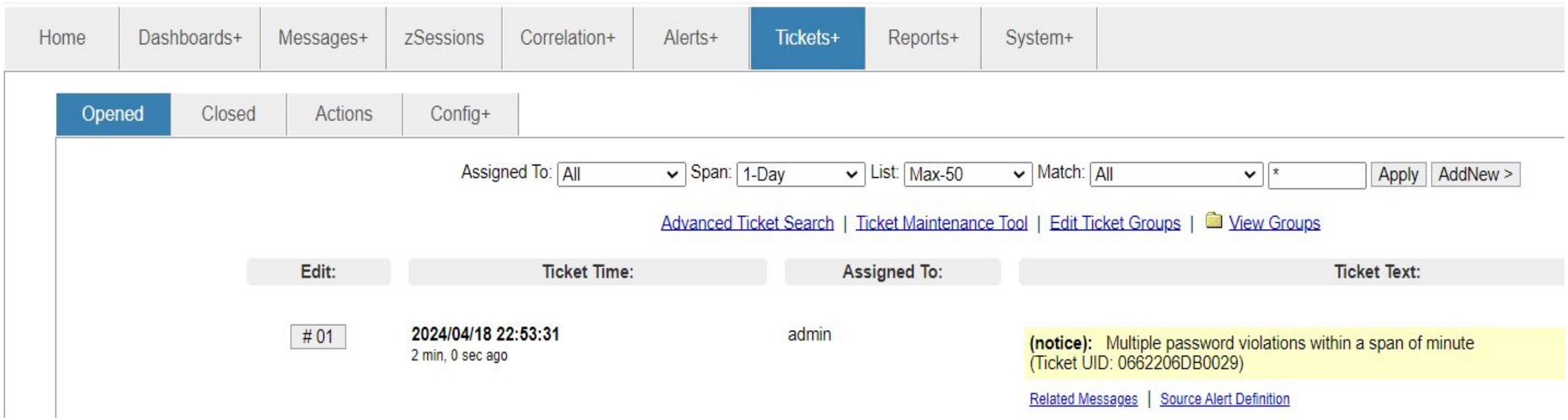


Security alerts for unauthorized access attempt

Security alert rule set up



Alerts created



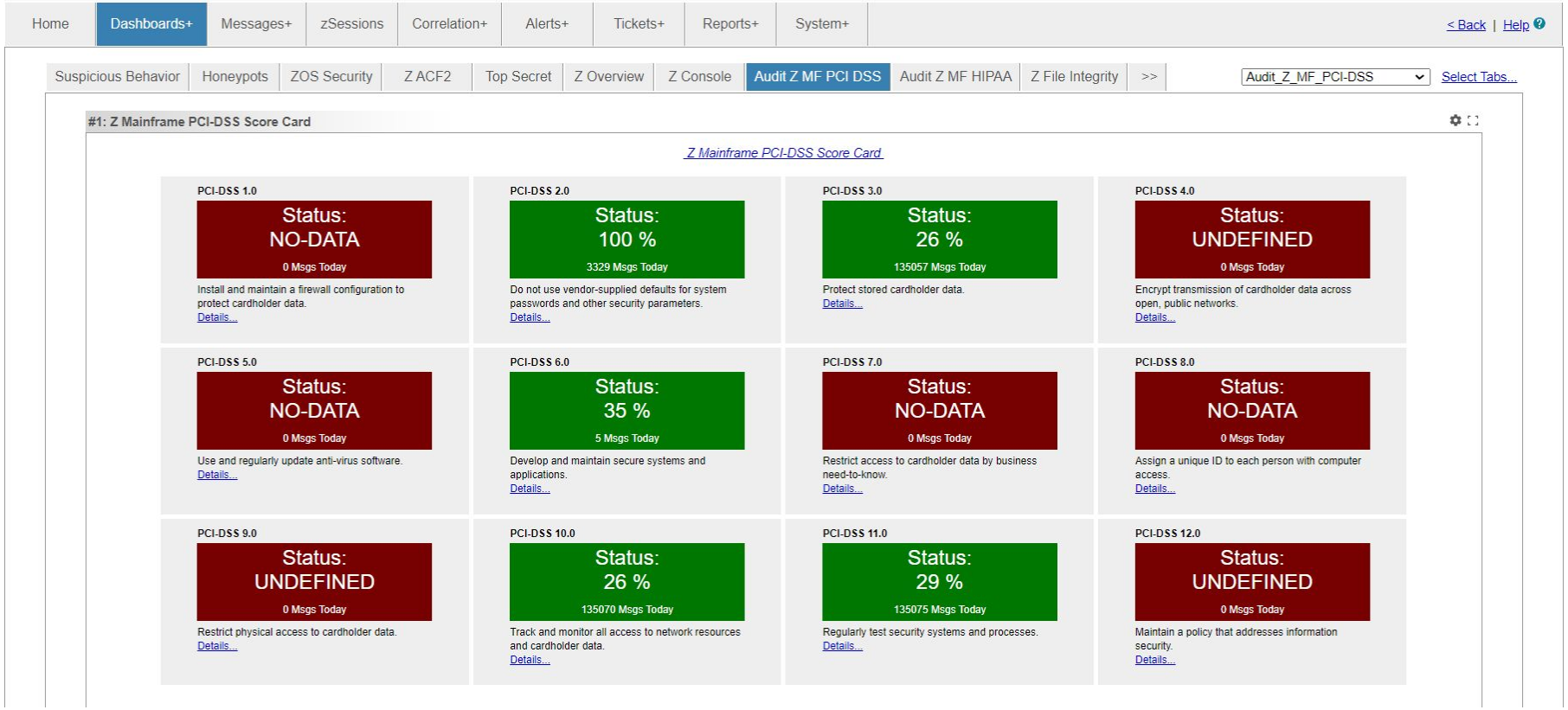
Compliance

PCI DSS
GDPR
HIPAA
FISMA

GLBA
NERC
FERC

Sarbanes-Oxley
ISO 27001
IRS Pub. 1075

Analytics engine showing PCI DSS compliance details



Analytics engine showing PCI DSS compliance details (continued...)

Score Card Report Name	Z Mainframe PCI-DSS Score Card
Score Card Item Description	PCI-DSS 2.0 Do not use vendor-supplied defaults for system passwords and other security parameters.
Messages Today	5313 messages.
Messages Yesterday	10426 messages.
Messages Last 7 Days	15739 messages.
Messages Last 30 Days	15739 messages.
Message Daily Average	7869 messages.
Current Item Status	OK - Percent of Daily Avg: 67% Messages counts of the associated correlation threads indicate that sufficient data is being collected to validate that this compliance requirement is currently being satisfied.
Associated Correlation Threads	Z TSO Session Messages Z DB2 Administrative Actions

Time:	Address:	Facility:	Z TSO Session Messages:
2024/04/19 02:39:44 32 min, 57 sec ago	123.123.123.123 xyz.xyz.com	audit	**(info):** Apr 19 09:39:45 SYSM IMS_1_3: SAF: 1 - SAFD: RACF - IMSID: RD1P - * * * MainSeg: 03 - LogType: 03 - LogDesc: Output Message - Length: 847 - MSGFLAGS: {Last Msg, First Msg} - Flags2: 82 - Flags: {MSGSACMD, MSGFPRSP} - RespMode: Yes - SysSeg_Exists: Yes - MSG_Record_Num: 0800003c - Record_Num: 0800003c - Prefix_Length: 1112 - Flags3: {MSGF3NOE} - ENQ_Bypsd: Yes - UnitOfWork: d9c4f1d7e7d9c640cdbf4b20e643ca63d9c4f1d7e7d9c640cdb f4b20e95f4f5a0000 - ORIG_IMSID: RD1PXRF - ORIG_Stock_Clock: 2014-09-12T20:48:46.319 - PROC_IMSID: RD1PXRF - PROC_Stock_Clock: 2014-09-12T20:48:46.331 - * * * SysSeg: 81 - ID: 81 - Length: 64 - FLAG2: {MSGC2EPH, MSGC2MSC, MSGC2MFS} - MFS_Exist: Yes - MSC_Exists: Yes - EP_Exit: Yes - FLAG3: {MSGC3MAT} - MSG_Time: Yes - SEQ: 10978 - OUTPUT_NUM: 1 - Switches: 1 - LU6_Type: 4.26G - LU6_Addr: 1.29G - * * * ExtPrefSeg: 86 - ID: 86 - Length: 16 - Data: Data: - Prefix_Length: 984 - Ext_Exist: {MSGETMR, MSGEMEX, MSGESEX, MSGEWLM, MSGESEC, MSGEAPPC} - APPC_Exists: Yes - SEC_Exists: Yes - WLM_Exists: Yes - SSE_Exists: Yes - MSC_SE_Exists: Yes - TMR_SegItem_Exists: Yes - * * * SecSeg: 88 - ID: 88 - Length: 22 - Data: Data: - UserID: RIHJER2 - Userid_Ind: UserID - * * * MSF_Ext: 8b - SegID: 8b - SIDS: Yes - MSCSource: fdfffffff4ca93360 - OrigIMSID: RD1PXRF - OrigToken: 2014-09-12T20:48:46.319 - CopyPRID: RD1PXRF - * * * MSC_TMR: 8c - Length: 144 - SegID: 8c - TimeStamp: 1970-01-01T12:00:00.000 - DestName: 11254 - Lterm: fdfffffff4ca93360 - DestSID: 1 - OrigSID: 1 - MSFlag1: MSG1RESP - MSFlag2: {MSG2DEST} - Destination: Yes - MSFlag3: {MSG3DLI, MSG3RSPM} - RespMode: Yes - DLI: Yes - MSFlag4: {MSG4XTFX} - HasExtPF: Yes - IMSRlse: 13 - IMSMod: 10 - IMSHWRel2: 13 - IMSHWMod2: 10 - * * * Text: 90 - Length: 184 - TEXTData: SYMQEC20 'THIS IS A TEST OF SYMQECHO VIA TCPIC. WITH SOME LUCK, I 'LL BE ABLE TO SEND A LONGER MESSAGE FROM THE TSO BATCH JOB THAT IS RUNNING TCPIC, WHICH IS A REXX PROGRAM. ' Details...

Processing reports

```
IMSLOG10,IMSID,LOGRC_LENGTH,LOGRC_TYPE,LOGRC_STCK,LOGRC_SEQUENCE_NUMBER,SCBTAMT,SCVTAMT,SCAOI,SCERROR,SCERROR_TEXT,SCCMD,SCLINE,SCTE
IMSLOG10,Char,Integer,Hex,Timestamp,Hex,Y/N,Y/N,Y/N,Integer,Char,Char,Integer,Integer,Char,Char,Timestamp,Char
IMSLOG16,IMSID,LOGRC_LENGTH,LOGRC_TYPE,LOGRC_STCK,LOGRC_SEQUENCE_NUMBER,SGNTCPIP,SGNVTAM,SGNBTAM,SGNISCAL,SGNOFFRC,SGNOFF,SGNON,SGNA
IMSLOG16,Char,Integer,Hex,Timestamp,Hex,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Y/N,Char,Char,Char,Char,Timestamp
IMSLOG10,IMS1,60,10,2021049183040278789,0000000000000169,N,Y,N,4,"USER OR TRAN NOT DEFINED TO RACF",,,,VT000049,USER,202104918304027
IMSLOG10,IMS1,60,10,2021049183042200509,000000000000016A,N,Y,N,4,"USER OR TRAN NOT DEFINED TO RACF",,,,VT000049,USER2,20210491830422
IMSLOG10,IMS1,60,10,2021049183043842284,000000000000016B,N,Y,N,4,"USER OR TRAN NOT DEFINED TO RACF",,,,VT000049,USER3,20210491830438
IMSLOG10,IMS1,60,10,2021049183046444326,000000000000016C,N,Y,N,4,"USER OR TRAN NOT DEFINED TO RACF",,,,VT000049,USER4,20210491830464
IMSLOG10,IMS1,60,10,2021049183408582431,000000000000016D,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000049,U
IMSLOG10,IMS1,60,10,2021049183412024252,000000000000016E,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000049,U
IMSLOG10,IMS1,60,10,2021049183418537399,000000000000016F,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000049,U
IMSLOG10,IMS1,60,10,2021049183423576512,0000000000000170,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000049,U
IMSLOG10,IMS1,60,10,2021049183428048467,0000000000000171,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000049,U
IMSLOG10,IMS1,60,10,2021049183432132876,0000000000000172,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000049,U
IMSLOG10,IMS1,60,10,2021049183435750012,0000000000000173,N,Y,N,28,"USER'S ACCESS REVOKED",,,,VT000049,USER128C,2021049183435750001,
IMSLOG10,IMS1,60,10,2021049183440010741,0000000000000174,N,Y,N,28,"USER'S ACCESS REVOKED",,,,VT000049,USER128C,2021049183440010733,
IMSLOG10,IMS1,60,10,2021049183443983033,0000000000000175,N,Y,N,28,"USER'S ACCESS REVOKED",,,,VT000049,USER128C,2021049183443983024,
IMSLOG10,IMS1,60,10,2021049183459528990,0000000000000176,N,Y,N,28,"USER'S ACCESS REVOKED",,,,VT000049,USER128C,2021049183459528982,
IMSLOG10,IMS1,60,10,2021049183502862219,0000000000000177,N,Y,N,28,"USER'S ACCESS REVOKED",,,,VT000049,USER128C,2021049183502862208,
IMSLOG16,IMS1,80,16,2021049183510367545,0000000000000179,N,Y,N,N,N,N,Y,N,N,Y,N,N,N,Y,USER12,VT000049,CC105511,USER12,202104918351036
IMSLOG10,IMS1,60,10,2020087170922412900,00000000000001C8,N,Y,N,4,"USER OR TRAN NOT DEFINED TO RACF",,,,VT000004,USER1,20200871709224
IMSLOG10,IMS1,60,10,2020087170922427114,00000000000001C9,N,Y,N,8,"PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED",,,,VT000005,U
```

Processing reports (continued…)

IMSLOG10	IMSID	SCBTAMT	SCVTAMT	SCAOI	SCERROR	SCERROR_TEXT	SCCMD	SCLINE	SCTERM	SCNODE	SCTRAN	SCPGM
IMSLOG10	Char	Y/N	Y/N	Y/N	Integer	Char	Char	Integer	Integer	Char	Char	Char
IMSLOG16	IMSID	SGNTCPIP	SGNVTAM	SGNBTAM	SGNISCAL	SGNOFFRC	SGNOFF	SGNON	SGNASOFF	SGNALLOC	SGNONSEC	SGNARNR
IMSLOG16	Char	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N
IMSLOG10	IMS1	N	Y	N	4	USER OR TRAN NOT DEFINED TO RACF				VT000049	USER	
IMSLOG10	IMS1	N	Y	N	4	USER OR TRAN NOT DEFINED TO RACF				VT000049	USER2	
IMSLOG10	IMS1	N	Y	N	4	USER OR TRAN NOT DEFINED TO RACF				VT000049	USER3	
IMSLOG10	IMS1	N	Y	N	4	USER OR TRAN NOT DEFINED TO RACF				VT000049	USER4	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000049	USER12	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000049	USER121	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	28	USER'S ACCESS REVOKED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	28	USER'S ACCESS REVOKED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	28	USER'S ACCESS REVOKED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	28	USER'S ACCESS REVOKED				VT000049	USER128C	
IMSLOG10	IMS1	N	Y	N	28	USER'S ACCESS REVOKED				VT000049	USER128C	
IMSLOG16	IMS1	N	Y	N	N	N	N	Y	N	N	Y	N
IMSLOG10	IMS1	N	Y	N	4	USER OR TRAN NOT DEFINED TO RACF				VT000004	USER1	
IMSLOG10	IMS1	N	Y	N	8	PASSWORD NOT DEFINED TO USER OR USER NOT AUTHORIZED				VT000005	USER121	

Contacts

Product Developer - BMC IMS SYSADMIN products
Santosh Belgaonkar - santosh_belgaonkar@bmc.com

Sr. Product Developer - BMC IMS Database Utilities products
Sahil Gupta - sahil_gupta@bmc.com