

Safeguard your data, Sustain Compliance and Optimize Security Intelligence with zSecure

Session 16276

Lunch n Learn

Tuesday, August 5, 2014

Glinda Cummings

Sr. Security Product Manager

glinda@us.ibm.com



Have you talked to a 'mainframe' today?

- Did you withdraw cash out of a bank's ATM?
- Did you make a purchase at a major retail store?
- Did you make a bank to bank transfer locally or internationally?
- Did you make an airline ticket reservation?
- Did you apply for a credit card?



... at some point in these daily transactions, you likely touched a mainframe.

The Mainframe (System z) is The Platform Choice Of ...

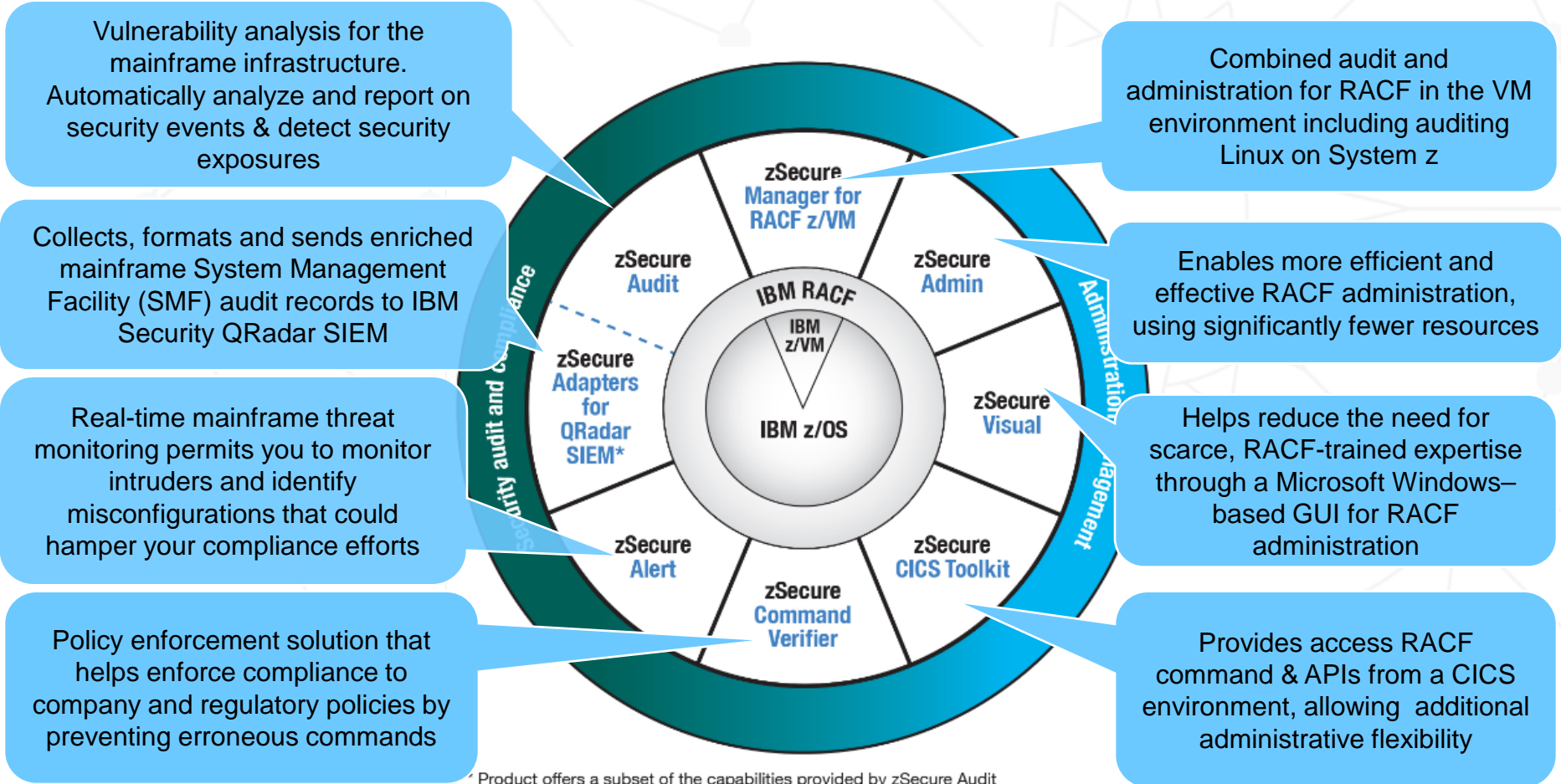
- 25 of the Top 25 Global Banks
- 110 of the Top WW 120 banks ranked by asset size
- 23 of the Top 25 U.S. Retailers
- 21 out of the Top 25 Insurance Organizations
- 9 Of The Top 10 Global Life/Health Insurance Providers



Have you been subject to a not so good audit result...



IBM Security zSecure helps address mainframe security challenges



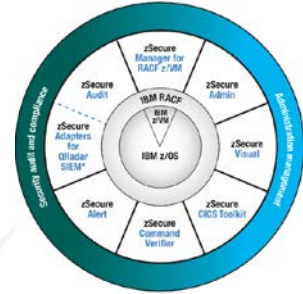
* Product offers a subset of the capabilities provided by zSecure Audit

* Supports RACF, CA ACF2 and CA Top Secret

** Supports RACF and CA ACF2

ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Enhanced compliance reporting



■ Features

- Extend automation and coverage for PCI-DSS*, STIG**, GSD331*** and other regulatory requirements
 - New reports specific to PCI-DSS, STIG
 - More flexible reporting
 - Ability to combine report types
 - Allow for exceptions
 - Target percentage reporting
 - Improved UI
 - Enhanced zoom in UI reporting

* PCI DSS: Payment Card Industry Data Security Standard for retail payments

** STIG: Security Technical Implementation Guide; Guidelines from US Defense Information Systems Agency (DISA)

*** GSD331: IBM's primary information security controls documentation for Strategic Outsourcing customers

■ Benefits

- Helps customers comply with latest iterations of regulations
- Helps customers identify, document, and remediate security breaches

Compliance reporting – Simple user interface

- Available as option AU.R

```
zSecure Suite - Audit - Compliance
Command ==> █
Compliance evaluation
- 1. STIG
- 2. GSD
- 3. Test a single rule (set) member
Compliance result selection
- Compliant      - Non-compliant      - Undecided
Output/run options
- Print format      Customize title      Send as e-mail
- Background run
```

- 1 - run all available STIG rules/tests
- 2 - run all available GSD331 rules/tests
- 3 - run individual rule
- Choose results to include in report (none=all)

Compliance reporting – Sample report

➤ Example Output:

```
IBM Security zSecure COMPLIANCE summary
Command ==> █
Standard      Cmp Non
MyStd         64 35
Domain name   Cmp Non
__ APFlibs    65 34
__ LNKlist    64 36
__ LPAlist    64 35
```

➤ Zoom in

```
Standard      Cmp Non
MyStd         64 35
Domain name   Cmp Non
APFlibs       65 34
Rule          Cmp Non
APF_profile   65 34
Test name     Cmp Non
__ failure_audit 95 5
__ success_audit 2 97
__ uacc       100 0
```

➔ We're good at access, but not so good at auditing

Compliance reporting – Sample output RACF

```

Standard compliance test results                                     Line 13 of 50
Command ==> _____ Scroll==> CSR
                                current settings
Complex Ver      Standards NonComp Unknown Exm Sup
LPAR400J          1          1          1    1
Standard
RACF_STIG        50          30          7    2    6.15
Rule set
ITNT0060 -       1          1          1
RACF0244         1
RACF0246         1
RACF0248         1
RACF0250         1
RACF0260        196          2
RACF0270         2
RACF0280         1
RACF0290         1
RACF0310        196          13          6
RACF0320        196          13          6
RACF0330         1
RACF0350         1
RACF0360         1          1
RACF0370         1
RACF0380         1
Description
SMF recording options for
FACILITY resource class m
The OPERCMDS resource cla
MCS consoles must be acti
The Automatic Data Set Pr
All active classes must b
The CLASSACT SETROPTS mus
The CMDVIOL SETROPTS valu
The EGN SETROPTS value mu
The GENCMD SETROPTS value
The GENERIC SETROPTS valu
The TERMINAL SETROPTS val
The GRPLIST SETROPTS valu
The INACTIVE SETROPTS val
The INITSTATS SETROPTS va
The JES(BATCHALLRACF) SET

```

✓ RULE and RULE_SET names indicate compliant state

Compliance reporting – Zoom in to test level

```

Standard compliance test results                                     Line 1 of 4
Command ==> _____ Scroll==> CSR
                                current settings
Complex Ver Standards NonComp Unknown Exm Sup
LPAR400J          1          1          1  1
Standard Rule sets NonComp Unknown Exm Sup Version
RACF_STIG         50          30          7  2  6.15
Rule set Objects NonComp Unknown Exm Sup Description
RACF0244          1          FACILITY resource class m
Non Unk Exm Class System Type VolSer Resource
CLASS
Cmp Non Unk Ex Test name Test description Tests for object
--- Cmp b.1a.FACILITY_ACTIVE FACILITY class is active.
--- Cmp b.1b.FACILITY_GENERIC GENERIC must be enabled.
--- Cmp b.1c.FACILITY_GENCMD GENCMD must be enabled.
--- Cmp b.1d.FACILITY_RACL FACILITY class must be RACLISTed.
***** Bottom of Data *****
    
```

✓ Test names contain clear test numbers

Compliance reporting – Zoom in to detail level

```

Standard compliance test results                                     Line 1 of 53
Command ==> _____ Scroll==> PAGE
                                current settings

Object tested
Complex name                LPAR400J
System name
Test domain newlist type   class
Object type or resource class CLASS
Object or resource name    FACILITY
Profile or data set type

Test definition
Test name                   b.1a.FACILITY_ACTIVE
Test lookup base field name
Test field name            ACTIVE
Relational operator       =
Compliance comparison value Yes
Test result
Test is true                Yes
Test value is compliant    Yes
Non-compliant audit finding No
Exempt from rule           No
Lookup against
Actual value of test field Yes
Domain
Domain name                FACILITY_class
Domain description
    
```

Audit priority derived from severity

- Extra **SEVERITY** keyword on the RULE and RULE_SET statement: `[SEVERITY({1 | 2 | 3 | HIGH | MEDIUM | LOW})]`
- New **SITE_SEVERITY** statement for RULE (SET) and COMPLEX
- Non-compliant rules receive an **AUDITPRIORITY**, based on
 - Default value **20**
 - RULE or RULE_SET severity
 - SITE_SEVERITY for RULE or RULE_SET
 - Increase/Decrease **10** using SITE_SEVERITY for COMPLEX
- Declare a rule not applicable for your environment or complex

AU.R – STDETAIL Zoomable compliance test details

Standard compliance test results Line 1 of 92

Command ==> _____ Scroll==> CSR

30 Jun 2014 07:46

Complex	Ver	Pr	Standards	NonComp	Unknown	Exm	Sup	Version
NM87	NM87	30	1					
Standard		Pr	Rule sets	58	3	4		6.19
RACF_STIG		30	92					
Rule set		Pr	Objects	NonComp	Unknown	Exm	Sup	Caption
___ AAMV0030		20	1	1				LNKAUTH=APFTAB
___ AAMV0040		10	630	101				APF libraries exist
___ AAMV0050			14					APF libraries unique
___ AAMV0160		20	132	26				PPT programs exist
___ AAMV0380			4					SMF record (sub)types
___ ACP00010		30	9	8				PARMLIB protected
___ ACP00020		20	7	5				Update on SYS1.LINKLIB
___ ACP00030		30	7	5				Update on SYS1.SVCLIB
___ ACP00040			1					Update on SYS1.IMAGELIB
___ ACP00050		30	7	5				Update on SYS1.LPALIB
___ ACP00060		30	62	48				Update+alter on APF list
___ ACP00070		30	69	59				Update+alter on LPA list
___ ACP00080		30	7	5				Update+alter on Nucleus
___ ACP00110		20	19	13				Update+alter on Linklist
___ ACP00170		30	5	4				RACF db protected
___ ACP00250		20	25	17				JES data sets protected
___ ACP00260		30	9	8				UADS protected
___ ACP00350		20	15	13				PROCLIBs protected
___ IFTP0020		30	2	2				FEARD profile protection
___ IFTP0030		30	1					FTP parm and JCL
___ IFTP0060		30	1					FTP config statements
___ IFTP0090		20	1	1				FTP SMF recording
___ ISLG0010		30	2					TFTP protected
								Syslogd init time

Narrow captions

Work!

Priority

AU.R – STDRULES Rule set overview by security DB

Standard rule set compliance summary

Line 1 of 110

Command ==>

Scroll==> CSR

27 Jun 2014 01:10

Complex	Ver	Pr	Standards							
NM84	NM84	30	1							
Standard		Pr	Rule sets							
RACF_STIG		30	110							
Rule set		Pri	Cm%	NS	TestPnt	Compli	NonCom	Unknow	Caption	
___ AAMV0030		20	0		1	0	1	0	LNKAUTH=APFTAB	
___ AAMV0040		30	84		632	534	98	0	APF libraries exist	
___ AAMV0050			100		14	14	0	0	APF libraries unique	
___ AAMV0160		20	80		132	106	26	0	PPT programs exist	
___ AAMV0380			100		280	280	0	0	SMF record (sub)types	
___ ACP00010		30	27		11	3	8	0	PARMLIB protected	
___ ACP00040			44		9	4	5	0	Update on SYS1.LINKLIB	
___ ACP00040			44		9	4	5	0	Update on SYS1.SVCLIB	
___ ACP00040		30	36		11	4	7	0	Update on SYS1.IMAGEL	
___ ACP00050		30	44		9	4	5	0	Update on SYS1.LPALIB	
___ ACP00060		30	40		135	54	81	0	Update+alter on APF l	
___ ACP00070		30	12		127	16	111	0	Update+alter on LPA l	
___ ACP00080		30	44		9	4	5	0	Update+alter on Nucle	
___ ACP00110		20	16		73	12	61	0	Update+alter on Linkl	
___ ACP00120		30	42		7	3	4	0	RACF db protected	
___ ACP00130		30	0		3	0	3	0	Master Catalog protec	
___ ACP00135		20	7		91	7	84	0	User Catalogs protect	
___ ACP00150		20	30		26	8	18	0	JES data sets protect	
___ ACP00170		30	27		11	3	8	0	UADS protected	
___ ACP00180		20	57		7	4	3	0	SMF data sets protect	
___ ACP00230		20	0		1	0	1	0	PAGE data sets protec	
___ ACP00250		30	12		16	2	14	0	PROCLIBs protected	
___ ACP00260		20	0		10	0	10	0	IEAABD profile protec	
___ ACP00350			100		0	0	0	0	IEASYMUP protection	
___ IFTP0020			100		3	3	0	0	FTP startup parm and	

Percentage

Rule set display – PCI-DSS example

```

Standard compliance test results                2 s elapsed, 1.9 s CPU
Command ==> CSR                               Scroll==> CSR
                                           10 Apr 2014 02:00
Complex Ver Pr Standards NonComp Unknown Exm Sup
SYS1      20      1      1      1      1
Standard Pr Rule sets NonComp Unknown Exm Sup Version
RACF-PCI-DSS 20      12      8      3      1      2.0
Rule set Pr Objects NonComp Unknown Exm Sup Caption
___ 1.2.1 20      1      1
___ 10.2.2 20      250      245
___ 10.2.5      1      1
___ 2.2.2      1      1
___ 7.2.3 20      2432      222
___ 8.1 20      21      3      1
___ 8.4 20      2      1      1
___ 8.5.10 20      1      1
___ 8.5.12      1
___ 8.5.13      1
___ 8.5.5 20      1      1
___ 8.5.9 20      1      1
Restrict network traffic
Log root/admin actions
Log ident/authentication
Insecure services
Default deny all
Unique user id
Encrypt passwords
MINIMUM PASSW LEN(>=7)
SETROPTS PASSW HIST(>=4)
SETROPTS PASSW REVOK(<=6)
SETROPTS INACTIVE(90)
SETROPTS PASSW INT(<=90)
***** Bottom of Data *****
    
```

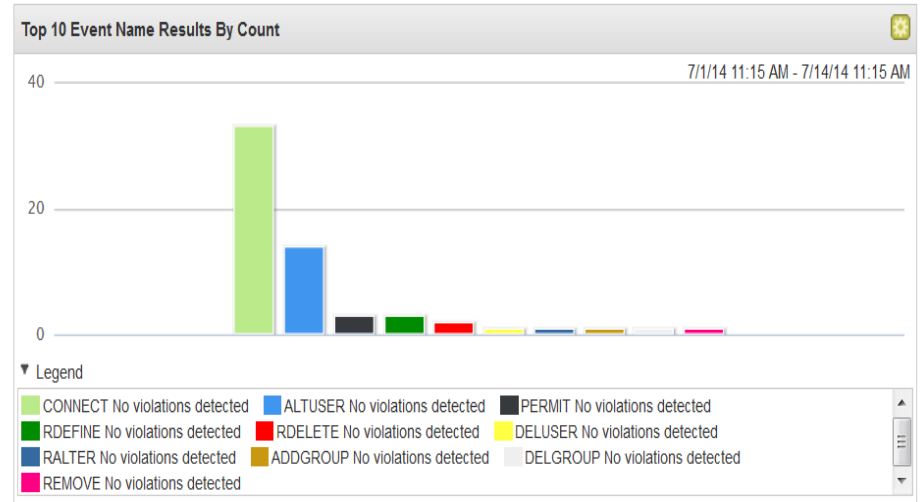
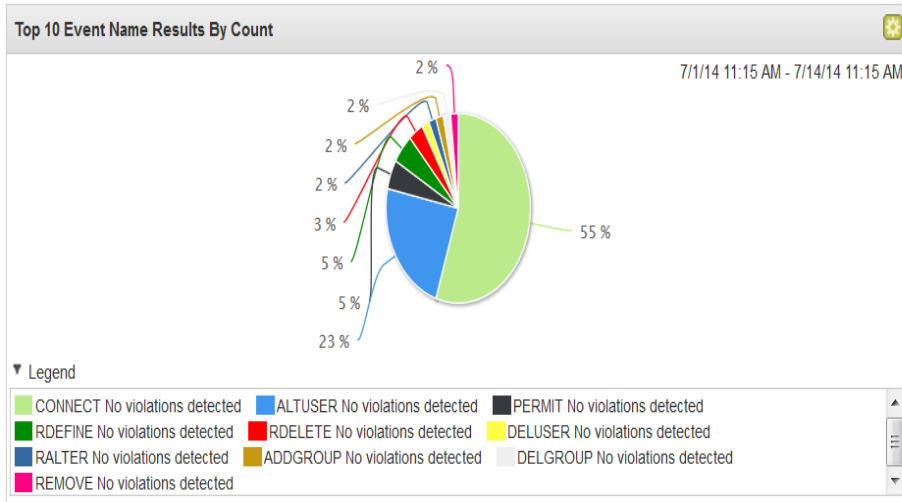
How about if you could transform this . . .

```
Audit Reporting Suite 30Jun14 09:30 to 13Jul14 16:30
```

```
RACF Command Activity
```

User	Count	Date	Time	RACF cmd
PEASEJ	69			
		30Jun	09:30	ALTUSER PEASEJ SPECIAL
		30Jun	09:39	ALTUSER PEASEJ SPECIAL
		30Jun	12:32	ALTUSER PEASEJ SPECIAL
		1Jul	10:35	ADDUSER DEMOUSER AUTHORITY(USE) DFLTGRP(SYSPROG) N
		1Jul	10:35	ALTUSER DEMOUSER NOOIDCARD NOPASSWORD RESUME
		1Jul	10:35	CONNECT DEMOUSER AUTHORITY(USE) GROUP(SYSPROG) NOA
		1Jul	10:35	ADDSD 'DEMOUSER.WORK.*' NOSET OWNER(SYSPROG)
		1Jul	10:35	PERMIT 'DEMOUSER.WORK.*' ACCESS(NONE) CLASS(DATASE
		1Jul	10:35	ALTDSD 'DEMOUSER.WORK.*' UACC(NONE)
		1Jul	10:35	RDEFINE SURROGAT (DEMOUSER.SUBMIT) LEVEL(0)
		1Jul	10:35	RALTER SURROGAT (DEMOUSER.SUBMIT) OWNER(DEMOUSER)
		1Jul	10:35	PERMIT DEMOUSER.SUBMIT ACCESS(READ) CLASS(SURROGAT

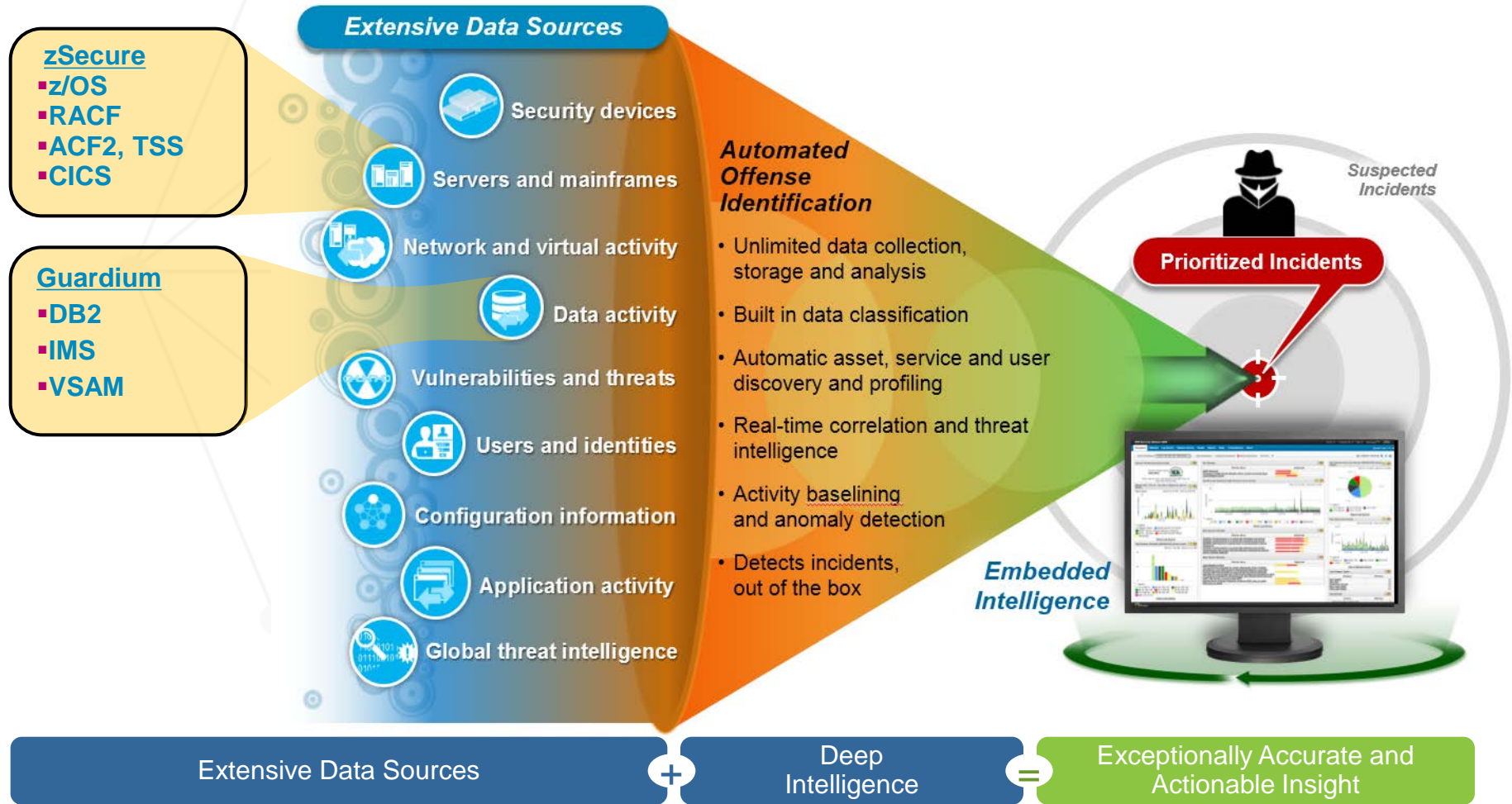
Into this . . .



(Hide Charts)

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count ▼
CONNECT No violations det...	Multiple (33)	7/1/14, 11:35:28 AM	PEASEJ	JAZZ03 RACF	Multiple (32)	Success	User Account Changed	33
ALTUSER No violations det...	Multiple (6)	7/1/14, 11:35:28 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	User Account Changed	14
PERMIT No violations detec...	Multiple (3)	7/1/14, 11:35:29 AM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDEFINE No violations dete...	Multiple (3)	7/1/14, 11:35:30 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDELETE No violations det...	Multiple (2)	7/1/14, 11:35:31 AM	Multiple (2)	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
DELUSER No violations det...	DELUSER DEMOUSER	7/1/14, 11:35:32 AM	PEASEJ	JAZZ03 RACF	DEMOUSER	Success	User Account Removed	1

Security intelligence automated offense identification for System z



Scenario # 1 – Inappropriate access to sensitive data on z/OS

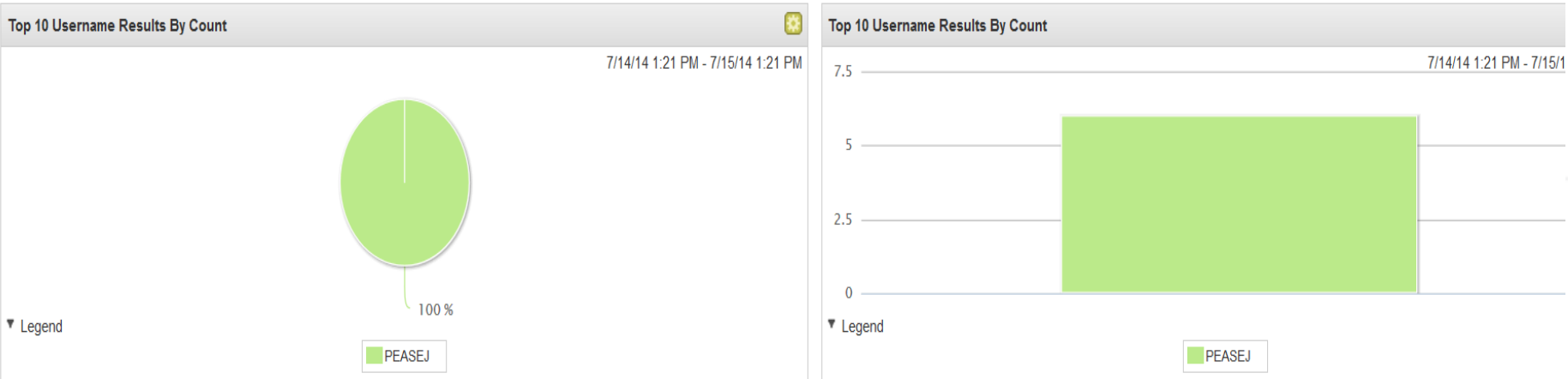
System Programmer
accesses a Payroll file on
System z

```

BROWSE      PAYROLL.EMPLOYEE.SALARY                               Line 00000000 Col 001 080
Command ==> _____ Scroll ==> CSR
***** Top of Data *****
U866ABC  GB046466  YN  63525  Payroll           London           £1,000,440
U866ACC  GB073535  YN  63525  Payroll           London           £  500,888
U866ACD  GB089985  YN  63525  Payroll           London           £   276,222
U866CXZ  GB027363  YN  63525  Payroll           London           £   172,142
U866HJJ  GB071333  YN  63525  Payroll           London           £2,320,440
U866HYT  GB022372  YY  58774  Internal Audit    London           £   442,888
U866IKY  GB099324  YN  58774  Internal Audit    London           £    76,222
U866JKO  GB063372  YN  45841  IT Operations     Leeds            £    72,345
U866JPD  GBCON883  NN  45841  IT Operations     Edinburgh        £    10,192
U866KYU  GB015553  YN  69844  Postal Services   London           £    55,388
U866NAY  GB055521  YY  23777  Fraud Team        Cardiff          £1,333,440
U866NAZ  GB035772  YN  23777  Fraud Team        Cardiff          £   500,891
U86603A  GB053533  YN  23777  Fraud Team        Cardiff          £   272,255
U866UNH  GB011413  YN  23777  Fraud Team        Cardiff          £   175,132
***** Bottom of Data *****

```

Scenario # 1 – Monitoring inappropriate access to sensitive data



(Hide Charts)

Username	Person name (Unique Count)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	SAF Class (Unique Count)	SAF resource name (Unique Count)	Access intent (Unique Count)	Access allowed (Unique Count)	Resource sensitivity (Unique Count)
PEASEJ	JAMIE PEASE	RACHECK Successf...	7/15/14, 12:10:08 PM	JAZZ03 RACF	DATASET	PAYROLL.EMPLOYEE.SALARY	Multiple (2)	ALTER	Sens read

Who accessed the sensitive resource

What they accessed

Resource is sensitive for read access

Scenario # 1 – Monitoring inappropriate access to sensitive data

Resource sensitivity (custom)	Sens read
SAF Class (custom)	DATASET
SAF resource name (custom)	PAYROLL.EMPLOYEE.SALARY
SNA terminal name (custom)	ISZ004
Sensitive groups (custom)	N/A
Sensitive user privileges (custom)	special auditor

Drill down into event detail

zSecure has enriched event data – assists the Security Officer to understand the user involved and what they accessed

Scenario # 2 – Privileged User Activities occurring on System z

Assigning powerful RACF attributes

```

zSecure Admin+Audit for RACF - Conf Command
Command ==>
Confirm or edit the following command
altuser U866ABC5 special
    
```

```

SETPROG APF,ADD,DSNAME=PEASEJ.LOADLIB,SMS
CSV410I SMS-MANAGED DATA SET PEASEJ.LOADLIB ADDED TO APF LIST
    
```

Modifying the Trusted Computing Base

Logon with powerful emergency user IDs

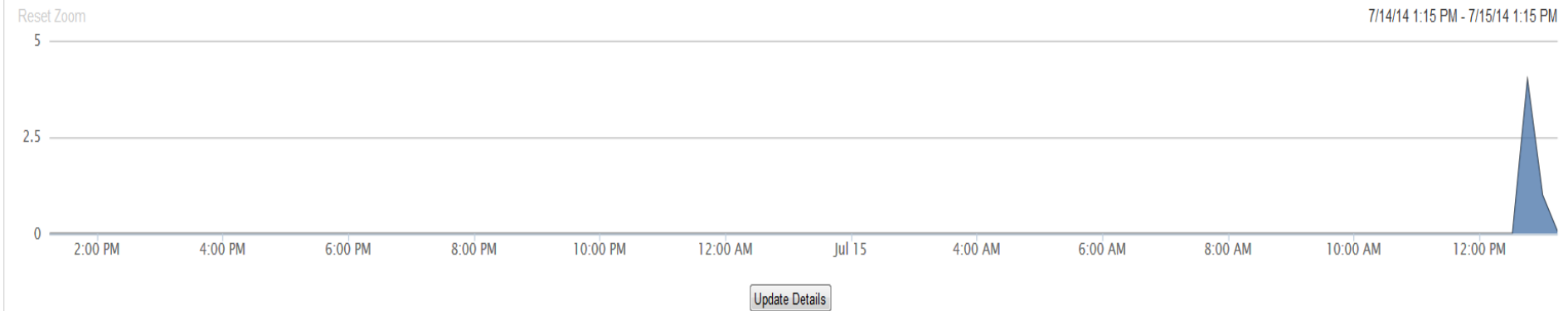
```

----- TS0/E LOGON -----
IKJ56714A Enter current password for EMERG01

Enter LOGON parameters below:                                RACF LOGON parameters:
Userid      ==> EMERG01
Password    ==> _                                           New Password ==>
    
```

Scenario # 2 – Monitoring Privileged User activities in QRadar

Records Matched Over Time



[\(Hide Charts\)](#)

Event Name	Log Source	Start Time ▼	Low Level Category	Username	AlertMsg
Logon_Emergency	JAZZ03 Alert	7/15/14, 1:13:26 PM	Admin Login Successful	EMERG01	Alert: Emergency user EMERG01 log...
Grant_Privilege_System	JAZZ03 Alert	7/15/14, 12:55:26 PM	User Right Assigned	PEASEJ	Alert: System authority granted to PE...
APF Data Removal	JAZZ03 Alert	7/15/14, 12:54:26 PM	System Configuration	N/A	Alert: Data set removal from APF list ...
Change_APF_List_Added	JAZZ03 Alert	7/15/14, 12:53:27 PM	Successful Configuration Modification	N/A	Alert: Data set added to APF list usin...
Change_APF_List_Removed	JAZZ03 Alert	7/15/14, 12:53:27 PM	Successful Configuration Modification	N/A	Alert: Data set removed from APF list...

Events sent to QRadar, seconds later

Collected and sent to QRadar by zSecure Alert

Scenario # 2 – Monitoring Privileged User activities in QRadar

Drill down into event detail

Event Information

Event Name	Logon_Emergency		
Low Level Category	Admin Login Successful		
Event Description	Logon by Emergency user.		
Magnitude	(2)	Relevance	1
Username	EMERG01		
Start Time	Jul 15, 2014, 1:13:26 PM	Storage Time	Jul 15, 2014, 1:13:26 PM
AlertMsg (custom)	Alert: Emergency user EMERG01 logged on - Successful logon or job submit with a userid meant for emergencies		

Source and Destination Information

Source IP	9.212.143.76	Destination IP	9.212.143.76
-----------	--------------	----------------	--------------

Detailed information alerts us to the fact that an emergency user ID has been used – big problem for mainframe customers!

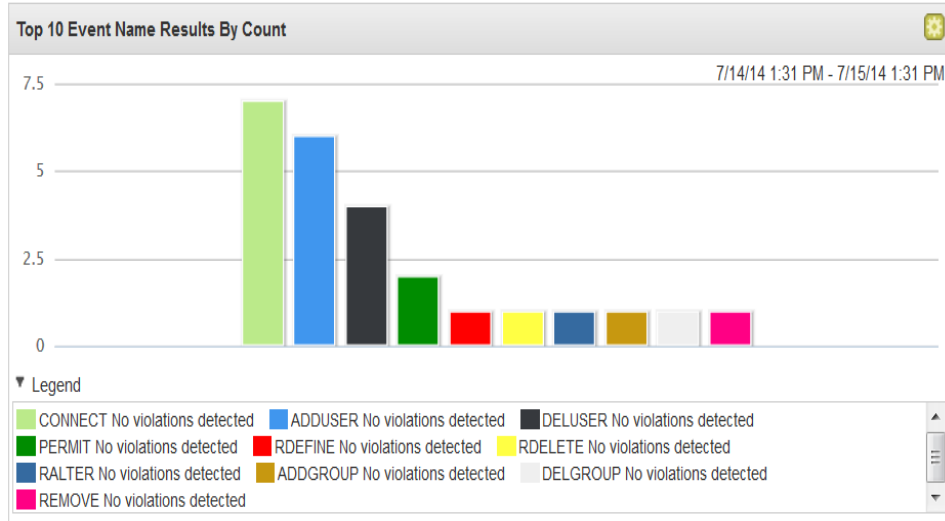
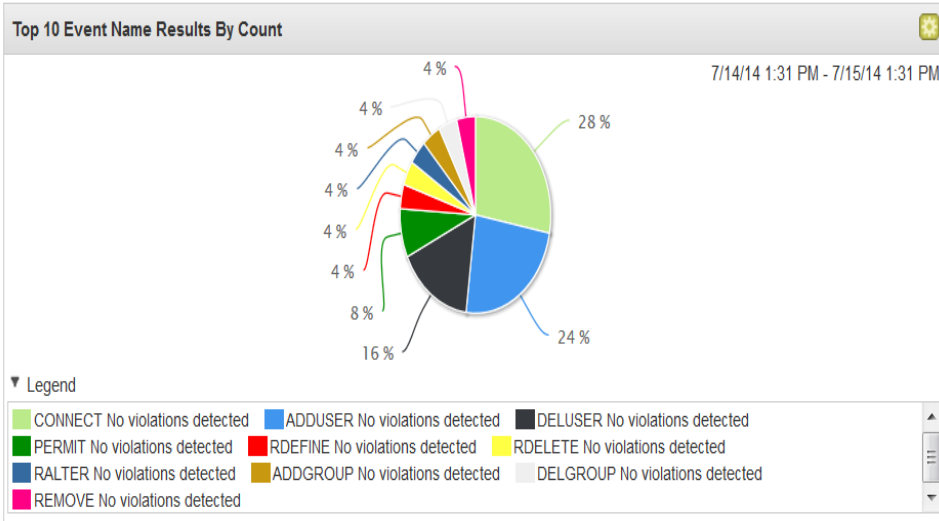
Scenario # 3 – Security Administrator activities occurring on System z

```
adduser demouser owner(sysprog) dfltgrp(sysprog) pass(1234yuds)
altuser demouser resume nopass nooid
connect demouser group(sysproc)
password user(demouser) interval(30)
addsd 'demouser.work.*' owner(sysprog)
permit 'demouser.work.*' id(demouser) acc(none)
altdsd 'demouser.work.*' uacc(none)
rdefine surrogat demouser.submit
ralter surrogat demouser.submit owner(demouser)
permit demouser.submit class(surrogat) id(sysprog)
addgroup testrob9 owner(sysprog) supgroup(sysprog)
altgroup testrob9 data('test group')
connect demouser group(testrob9)
```

Executing RACF
Commands

Security Administrator is
creating new security
definitions on the mainframe

Scenario # 3 – Monitoring Security Administrator activities



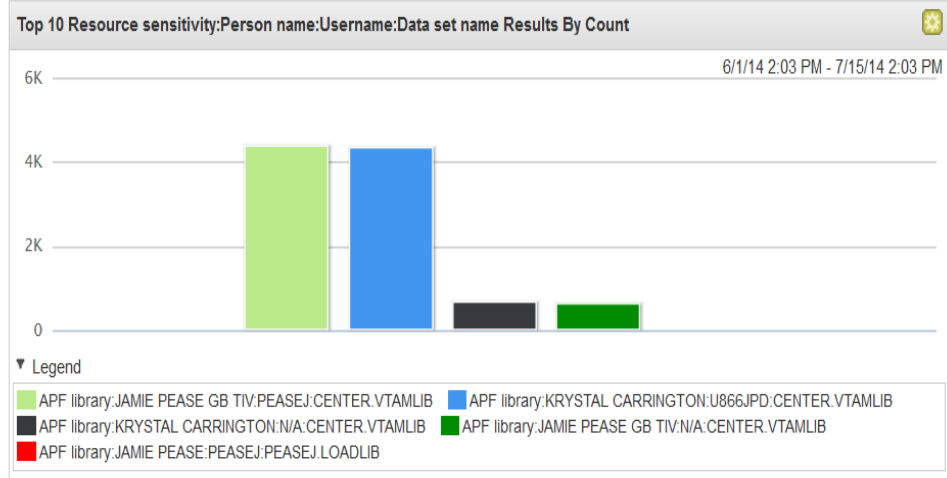
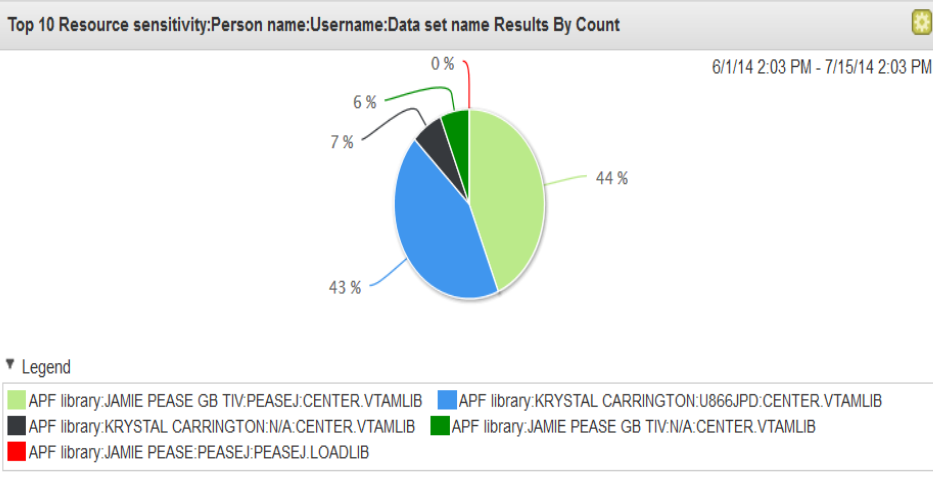
(Hide Charts)

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count
CONNECT No violations detected	Multiple (4)	7/14/14, 5:48:04 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	User Account Changed	7
ADDUSER No violations detected	Multiple (3)	7/14/14, 5:48:03 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	User Account Added	6
DELUSER No violations detected	Multiple (3)	7/14/14, 5:48:42 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	User Account Removed	4
PERMIT No violations detected	Multiple (2)	7/15/14, 12:50:26 PM	PEASEJ	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
RDEFINE No violations detected	RDEFINE SURROGAT (DE...	7/15/14, 12:50:26 PM	PEASEJ	JAZZ03 RACF	DEMOUSER.SUBMIT	Success	Policy Change	1

A view of the RACF commands that have been executed over a 24 hour period – mainframe customers typically run this type of report on a daily basis!

Event data collected by **zSecure Audit**

Scenario # 4 – Monitoring your System Programmers



(Hide Charts)

Resource sensitivity	Person name	Username	Data set name	Access intent (Unique Count)	Access allowed (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Job name (Unique Count)	Count
APF library	JAMIE PEASE GB TIV	PEASEJ	CENTER.VTAMLIB	UPDATE	ALTER	8/21/12, 6:39:10 PM	R IBM RACF 3	PEASEJ	4,374
APF library	KRYSTAL CARRINGTON	U866JPD	CENTER.VTAMLIB	UPDATE	ALTER	8/22/12, 4:14:16 PM	R IBM RACF 3	U866JPD	4,338
APF library	KRYSTAL CARRINGTON	N/A	CENTER.VTAMLIB	UPDATE	ALTER	6/24/14, 4:30:39 AM	R IBM RACF 3	U866JPD	668
APF library	JAMIE PEASE GB TIV	N/A	CENTER.VTAMLIB	UPDATE	ALTER	6/24/14, 4:30:22 AM	R IBM RACF 3	PEASEJ	631
APF library	JAMIE PEASE	PEASEJ	PEASEJ.LOADLIB	UPDATE	ALTER	7/2/14, 10:20:15 AM	JAZZ03 RACF	PEASEJ	1

Highly sensitive resource – keys to the kingdom!

Could be used to circumvent system security

Daily (scheduled) reporting

Customers typically run scheduled monitoring reports

!	Report Name ▲	Group	Schedule
	Access to Payroll files	Security	Daily
	Alerts from previous day	Security	Daily
	RACF Commands	Security	Daily
	RACF Violations	Security	Daily
	Sensitive Dataset Updates	Security	Daily

RACF Commands-1.pdf - Adobe Reader

File Edit View Window Help

1 (1 of 2) 50%

Tools Sign Comment

RACF Commands

Generated: Jul 2, 2014, 2:40:12 PM

RACF Commands
Z-RACF Commands
Jul 1, 2014, 12:00 AM GMT+2 - Jul 2, 2014, 12:00 AM GMT+2
Count

Legend:

- ALTUSER No violati...
- CONNECT No violati...
- PERMIT No violati...
- ADDSD No violatio...
- DELDSD No violati...
- ADDUSER No viola...
- REMOVE No violati...
- ADDGROUP No vib...
- ALTDSO No violati...
- ALTDSD No violati...
- ALTGROUP No viol...
- DELGROU No viol...
- RALTER No violati...
- RDELETE No violati...
- RDEFINE No violati...

RACF Commands Z-RACF Commands

Jul 1, 2014, 12:00:00 AM - Jul 2, 2014, 12:00:00 AM

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count
ALTUSER No violations detected	Multiple (2)	Jun 30, 2014, 10:30:01 AM	FEASEJ	JAZZ03 RACF	Multiple (2)	Success	User Account Changed	4
CONNECT No violations detected	Multiple (2)	Jul 1, 2014, 11:35:28 AM	FEASEJ	JAZZ03 RACF	DEMOUSER	Success	User Account Changed	2
PERMIT No violations detected	Multiple (2)	Jul 1, 2014, 11:35:29 AM	FEASEJ	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
ADDSD No violations detected	ADDSD 'DEMOUSER.WORK.X' NO SET OWNER(SYS PROG)	Jul 1, 2014, 11:35:29 AM	FEASEJ	JAZZ03 RACF	DEMOUSER.WORK.X	Success	Access Permitted	1
DELDSD No violations detected	DELDSD 'DEMOUSER.WORK.X'	Jul 1, 2014, 11:35:31 AM	FEASEJ	JAZZ03 RACF	DEMOUSER.WORK.X	Success	Policy Change	1

QRadar/zSecure – RACF – Access Violations by Resource

Welcome, admin [logout]

Dashboard Offenses Log Activity Network Activity Assets Reports Admin

System Time: 08:26 Preferences Help

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions Quick Filter...

Viewing events from 2012-08-25 09:00:00 to 2012-08-25 09:04:00 View: Select An Option: Display: Custom

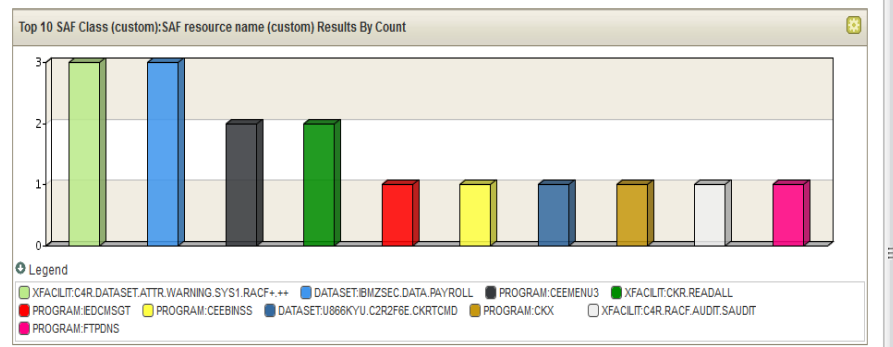
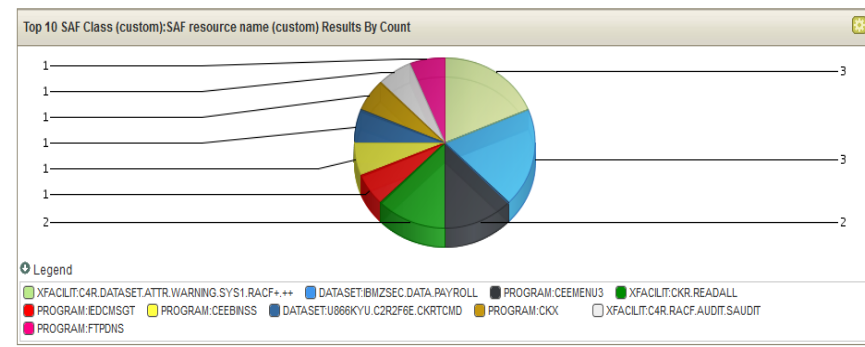
Grouping By: SAF Class (custom), SAF resource name (custom)

Using Search: RACF - Access Violations - By Resource

Current Filters: Log Source Group is IBM (Clear Filter), Event Name is RACHECK Insufficient authority (Clear Filter), Log Source is IBM RACF (Clear Filter)

Current Statistics

Completed



SAF Class (custom)	SAF resource name (custom)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Username (Unique Count)	Person name (custom) (Unique Count)	Event Count (Sum)	Access intent (custom) (Unique Count)	Access allowed (custom) (Unique Count)	Resource sensitivity (custom) (Unique Count)	Count
PROGRAM	CEEEMENU3	RACHECK Insufficient authority	11:12	IBM RACF	QRADFTP	Multiple (2)	45	READ	N/A	APF lib+Lnk	2
DATASET	U866KYU.C2R2F6E.CKRTCMD	RACHECK Insufficient authority	09:40	IBM RACF	U866ABC	DEX DEXTER	8	READ	N/A	N/A	1
XFACILIT	CKR.READALL	RACHECK Insufficient authority	07:58	IBM RACF	C2ECORLF	N/A	6	READ	N/A	N/A	2
XFACILIT	C4R.DATASET.ATTR.WARNING.SYS1.RACF+..	RACHECK Insufficient authority	09:38	IBM RACF	U866KYU	FALLON CARRINGTON	4	UPDATE	N/A	N/A	3
DATASET	IBMZSEC.DATA.PAYROLL	RACHECK Insufficient authority	08:42	IBM RACF	U866ABC	DEX DEXTER	3	READ	N/A	N/A	3
PROGRAM	IEDCMSGT	RACHECK Insufficient authority	11:12	IBM RACF	QRADFTP	QRADAR FTP USERID	1	READ	N/A	APF lib+Lnk	1
PROGRAM	CEEINSS	RACHECK Insufficient authority	11:12	IBM RACF	QRADFTP	QRADAR FTP USERID	1	READ	N/A	APF lib+Lnk	1
PROGRAM	CKX	RACHECK Insufficient authority	07:55	IBM RACF	C2ECORLF	N/A	1	READ	N/A	APF lib+Lnk	1
XFACILIT	C4R.RACF.AUDIT.SAUDIT	RACHECK Insufficient authority	09:16	IBM RACF	U866KYU	FALLON CARRINGTON	1	UPDATE	N/A	N/A	1
PROGRAM	FTPDNS	RACHECK Insufficient authority	11:12	IBM RACF	QRADFTP	QRADAR FTP USERID	1	READ	N/A	APF lib+Lnk	1
PROGRAM	CKRCARLA	RACHECK Insufficient authority	07:53	IBM RACF	C2ECORLF	N/A	1	READ	N/A	APF lib+Lnk	1

Displaying 1 to 11 of 11 items (Elapsed time: 0:00:00.116)

Copyright © 2012 Q1 Labs Inc. All rights reserved.

RACF Commands Issued

QRadar - Log Activity - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks ScrapBook Tools Help

QRadar - Log Activity

IBM Security QRadar SIEM admin Preferences Help IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin System Time: 20:58

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions Quick Filter...

Legend

- RACHECK Successful access
- AUDIT General event 0
- RACLINK No violations detected
- RACHECK Insufficient authority
- DEFINE Successful definition of profile
- PASSWORD No violations detected
- ALTUSER No violations detected
- DELETE Successful deletion of profile
- PERMIT No violations detected
- CONNECT No violations detected

Legend

- RACHECK Successful access
- AUDIT General event 0
- RACLINK No violations detected
- RACHECK Insufficient authority
- DEFINE Successful definition of profile
- PASSWORD No violations detected
- ALTUSER No violations detected
- DELETE Successful deletion of profile
- PERMIT No violations detected
- CONNECT No violations detected

(Hide Charts)

Event Name	Log Source Time (Minimum)	Log Source (Unique Count)	Username (Unique Count)	Person name (custom) (Unique Count)	Sensitive user privileges (custom) (Unique Count)	RACF authority used (custom) (Unique Count)	Command (custom) (Unique Count)	Category (Unique Count)	Count
RACHECK Successful acc...	2013-02-19 19:57:02	JAZZ03 RACF	Multiple (9)	Multiple (9)	Multiple (4)	Multiple (2)		Access Permitted	3,003
DEFINE Successful definiti...	2013-02-19 19:57:02	JAZZ03 RACF	Multiple (6)	Multiple (6)	Multiple (4)	Multiple (2)		Information	194
DELETE Successful deleti...	2013-02-19 19:57:14	JAZZ03 RACF	Multiple (5)	Multiple (5)	Multiple (3)	Normal		User Account Removed	188
AUDIT General event 0	2013-02-20 16:31:00	JAZZ03 RACF	Multiple (2)	Multiple (2)	special	N/A		General Audit Event	17
PASSWORD No violations ...	2013-02-21 17:07:14	JAZZ03 RACF	PEASEJ	JAMIE PEASE GB TIV	special	Special	PASSWORD PASSWORD(...	Information	14
ALTUSER No violations det...	2013-02-20 19:57:07	JAZZ03 RACF	Multiple (2)	Multiple (2)	special	Special	Multiple (5)	User Account Changed	6
RACLINK No violations det...	2013-02-21 17:09:19	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Multiple (2)	Multiple (2)	Information	5
PERMIT No violations dete...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	Multiple (2)	Information	4
CONNECT No violations d...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	Multiple (2)	Information	4
RACHECK Insufficient auth...	2013-02-21 17:06:10	JAZZ03 RACF	ROBVH3	ROB VAN HOBOKEN III	N/A	Normal		Unauthorized Access Attempt	3
SETROPTS No violations d...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	SETROPTS GENERIC(DAT...	Information	3
RALTER No violations dete...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	RALTER SURROGAT (ROB...	Information	2
ADDSD No violations detec...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	ADDSD 'ROBVH8.WORK.*' ...	Information	2
DELUSER No violations det...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	DELUSER ROBVH8	User Account Removed	2
DELGROUP No violations ...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	DELGROUP TESTROB9	Group Removed	2
DELDSD No violations det...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	DELDSD 'ROBVH8.WORK.*'	Information	2
ADDGROUP No violations ...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	ADDGROUP TESTROB9 O...	Group Added	2
ALTGROUP No violations d...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	ALTGROUP TESTROB9 DA...	Group Changed	2
ALTDSD No violations dete...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	ALTDSD 'ROBVH8.WORK.*'...	Information	2
ADDUSER No violations d...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	ADDUSER ROBVH8 AUTH...	User Account Added	2
REMOVE No violations det...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	REMOVE ROBVH8 GROUP...	Information	2
RDELETE No violations de...	2013-02-21 17:02:12	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	RDELETE SURROGAT (R...	Information	2
RDEFINE No violations det...	2013-02-21 17:02:11	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	Special	RDEFINE SURROGAT (RO...	Information	2
RACINIT Invalid password ...	2013-02-20 12:18:31	JAZZ03 RACF	ROBVH	ROB VAN HOBOKEN	special	N/A		General Authentication Failed	1
SETROPTS insufficient aut...	2013-02-21 17:06:10	JAZZ03 RACF	ROBVH3	ROB VAN HOBOKEN III	N/A	Normal	SETROPTS GENERIC(DAT...	Unauthorized Access Attempt	1
RDEFINE Insufficient autho...	2013-02-21 17:06:10	JAZZ03 RACF	ROBVH3	ROB VAN HOBOKEN III	N/A	Normal	RDEFINE SURROGAT (RO...	Unauthorized Access Attempt	1

Displaying 1 to 26 of 26 items (Elapsed time: 0:00:00.111)
© Copyright IBM Corp. 2012. All rights reserved.

Real Time Alerts from zSecure Alert

QRadar - Log Activity - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks ScrapBook Tools Help

QRadar - Log Activity

IBM Security QRadar SIEM admin Preferences Help IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin System Time: 18:09

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions Quick Filter...

Viewing events from 2013-02-21 17:04:00 to 2013-02-21 18:04:00 View: Select An Option: Display: Default (Normalized)

Current Filters:
Log Source is JAZZ03 Alert (Clear Filter)

Current Statistics

Total Results	5	Compressed Data Files Searched	0 (0B Total)	Duration	9ms
Data Files Searched	8 (53.7 KB Total)	Index File Count	60 (17.1 KB Total)		

Records Matched Over Time

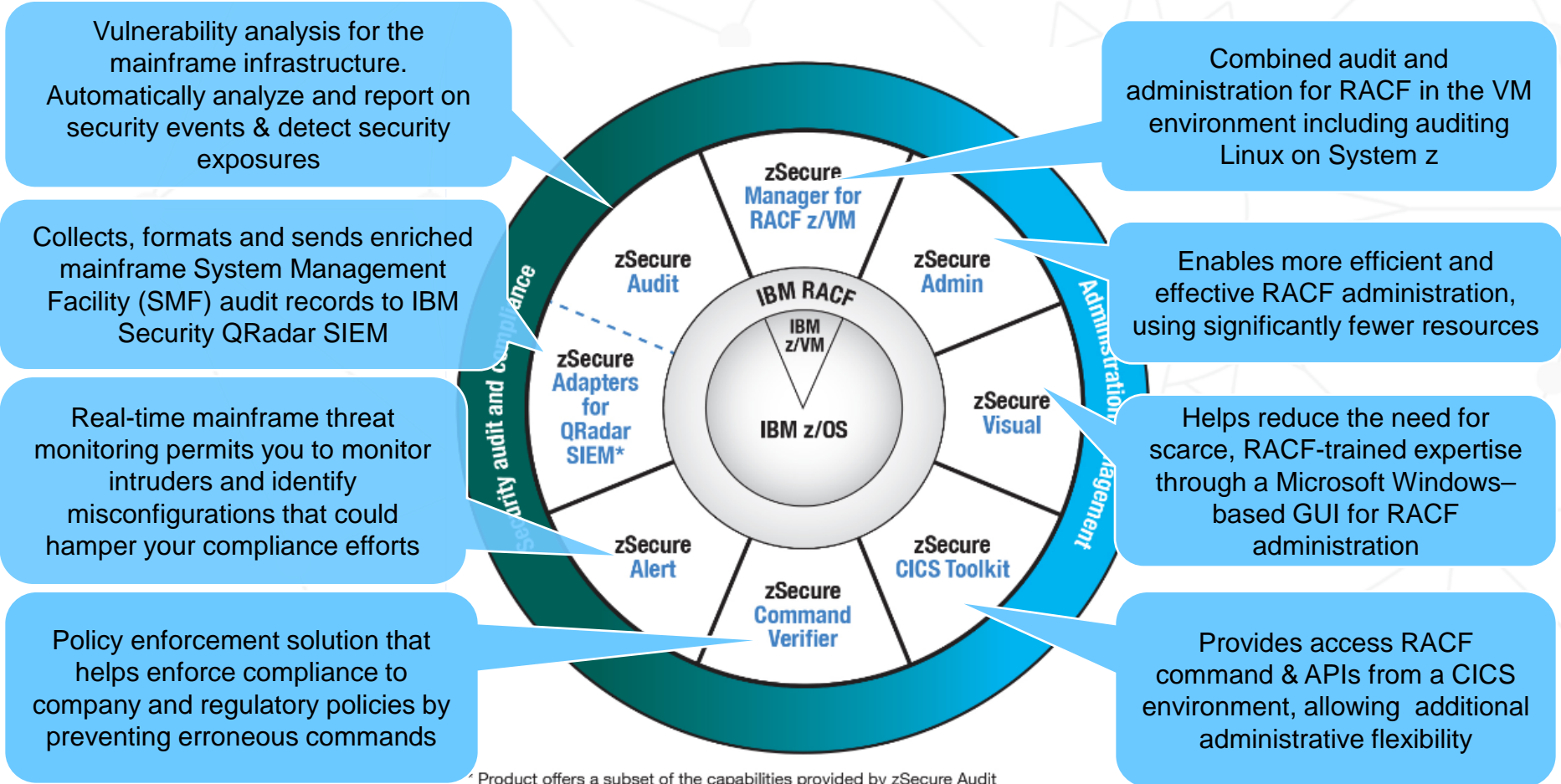
Update Details

(Hide Charts)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Revoke_Privilege_System	JAZZ03 Alert	1	2013-02-21 18:03:49	General Authentication Failed	9.212.143.76	0	9.212.143.76	0	ROBVH	3
Grant_Privilege_System	JAZZ03 Alert	1	2013-02-21 18:02:49	General Authentication Successful	9.212.143.76	0	9.212.143.76	0	ROBVH	3
unknown	JAZZ03 Alert	1	2013-02-21 17:13:39	Unknown	9.212.143.76	0	9.212.143.76	0	ROBVH	3
Change_APP_List_Removed	JAZZ03 Alert	1	2013-02-21 17:05:39	Successful Configuration Modifi...	9.212.143.76	0	9.212.143.76	0	N/A	3
Change_APP_List_Added	JAZZ03 Alert	1	2013-02-21 17:05:39	Successful Configuration Modifi...	9.212.143.76	0	9.212.143.76	0	N/A	3

Displaying 1 to 5 of 5 items (Elapsed time: 0:00:00.071)
© Copyright IBM Corp. 2012. All rights reserved.

IBM Security zSecure helps address mainframe security challenges



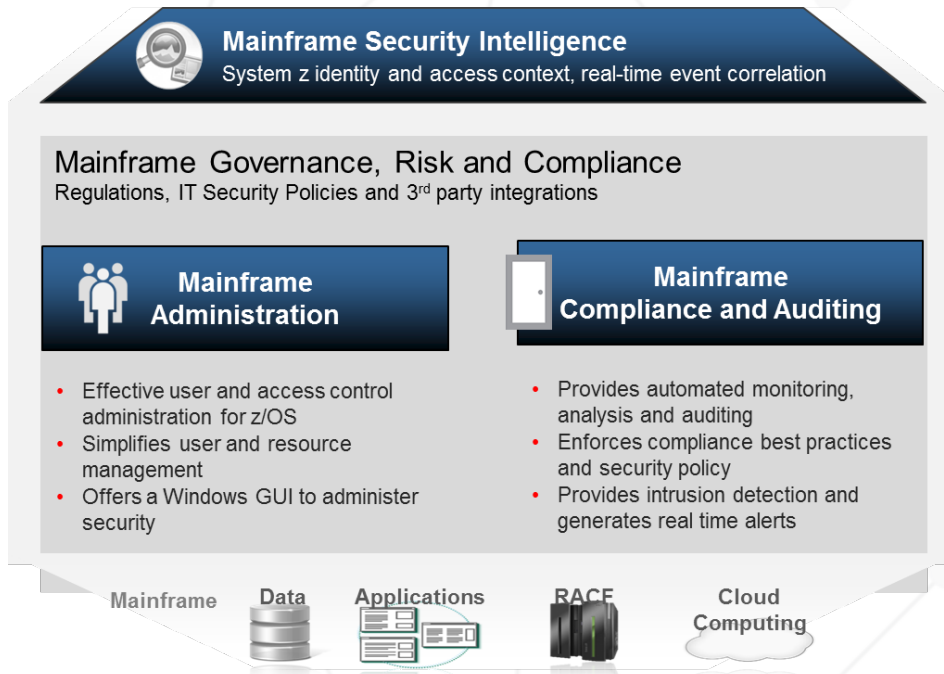
* Product offers a subset of the capabilities provided by zSecure Audit

* Supports RACF, CA ACF2 and CA Top Secret

** Supports RACF and CA ACF2

ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

What's new in zSecure suite 2.1.1

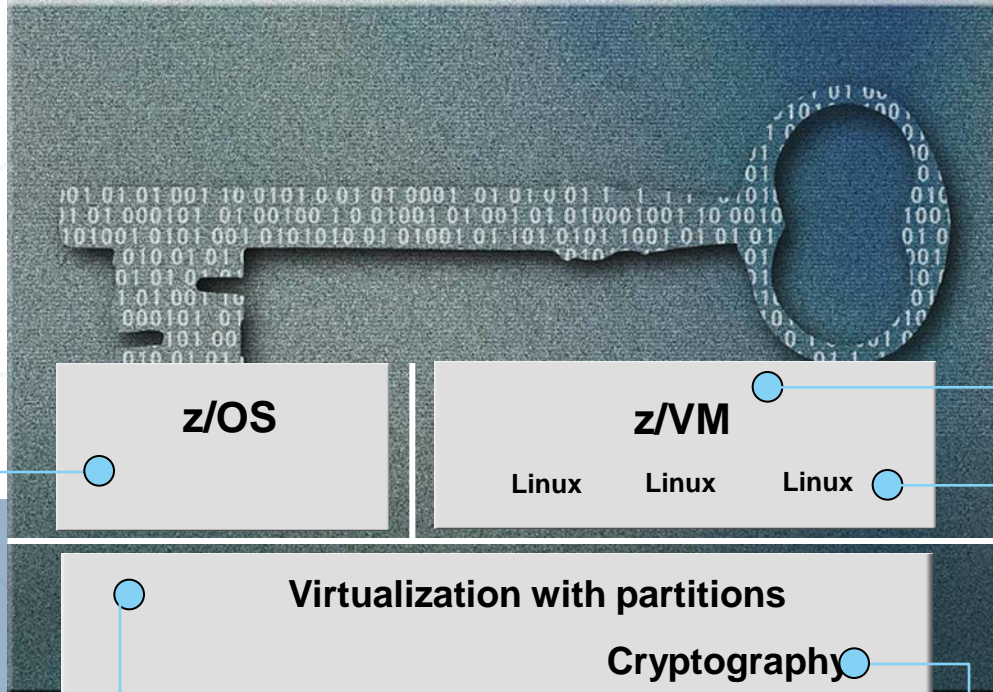


IBM security solution

- **IBM Security zSecure Suite 2.1.1**

- Compliance, auditing and monitoring – extending compliance framework for automation and coverage for compliance verification
 - PCI DSS requirements
 - STIG RACF and STIG ACF2 – increase our coverage of STIG auditing controls to increase automation
 - Add STIGplus (commercial version of STIG with additional subsystem alternatives)
- Integrated mainframe security intelligence
 - MQ Series – compliance requirements plus assign sensitivity levels to sensitive data sets and resources
 - Enhanced Guardium - Pass remaining object types to Guardium plus new object types for DB2 11
 - DB2 objects (i.e. complete SAF protected object set)
- IBM security software integration
 - QRadar SIEM – custom reporting for information from zSecure Audit, Add event mapping and custom fields for additional SMF records for example for MQ Series
- zSecure Adapters for Qradar SIEM - new product

System z Certifications



The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles

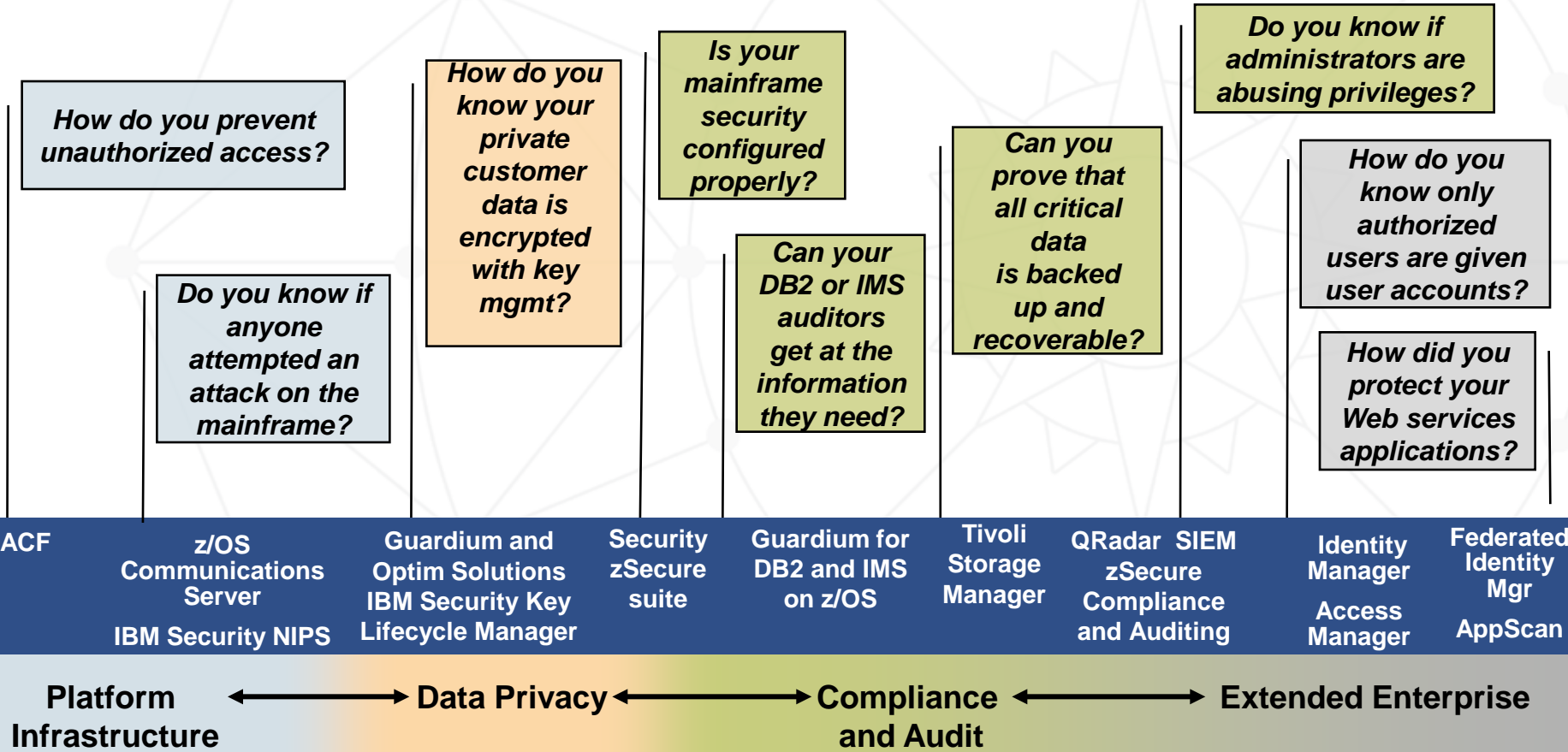
- ### z/VM
- Common Criteria
 - z/VM 6.1 is EAL 4+ for OSPP
 - z/VM 6.1 System SSL is FIPS 140-2 certified.
 - System Integrity Statement

- ### Linux on System z
- Common Criteria
 - SUSE SLES11 SP2 certified at EAL4+ with OSPP
 - Red Hat EL6.2 EAL4+ with CAPP and LSPP
 - OpenSSL - FIPS 140-2 Level 1 Validated
 - CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

- ### z/OS
- Common Criteria EAL4+
 - with CAPP and LSPP
 - z/OS 1.7 → 1.10 + RACF
 - z/OS 1.11 + RACF (OSPP)
 - z/OS 1.12 , z/OS 1.13 (OSPP)
 - Common Criteria EAL5+
 - RACF V1R12 (OSPP)
 - RACF V1R13 (OSPP)
 - z/OS 1.10 IPv6 Certification by JITC
 - IdenTrust™ certification for z/OS PKI Services
 - FIPS 140-2
 - System SSL z/OS 1.10 → 1.13
 - z/OS ICSF PKCS#11 Services - z/OS 1.11 → z/OS 1.13
 - Statement of Integrity

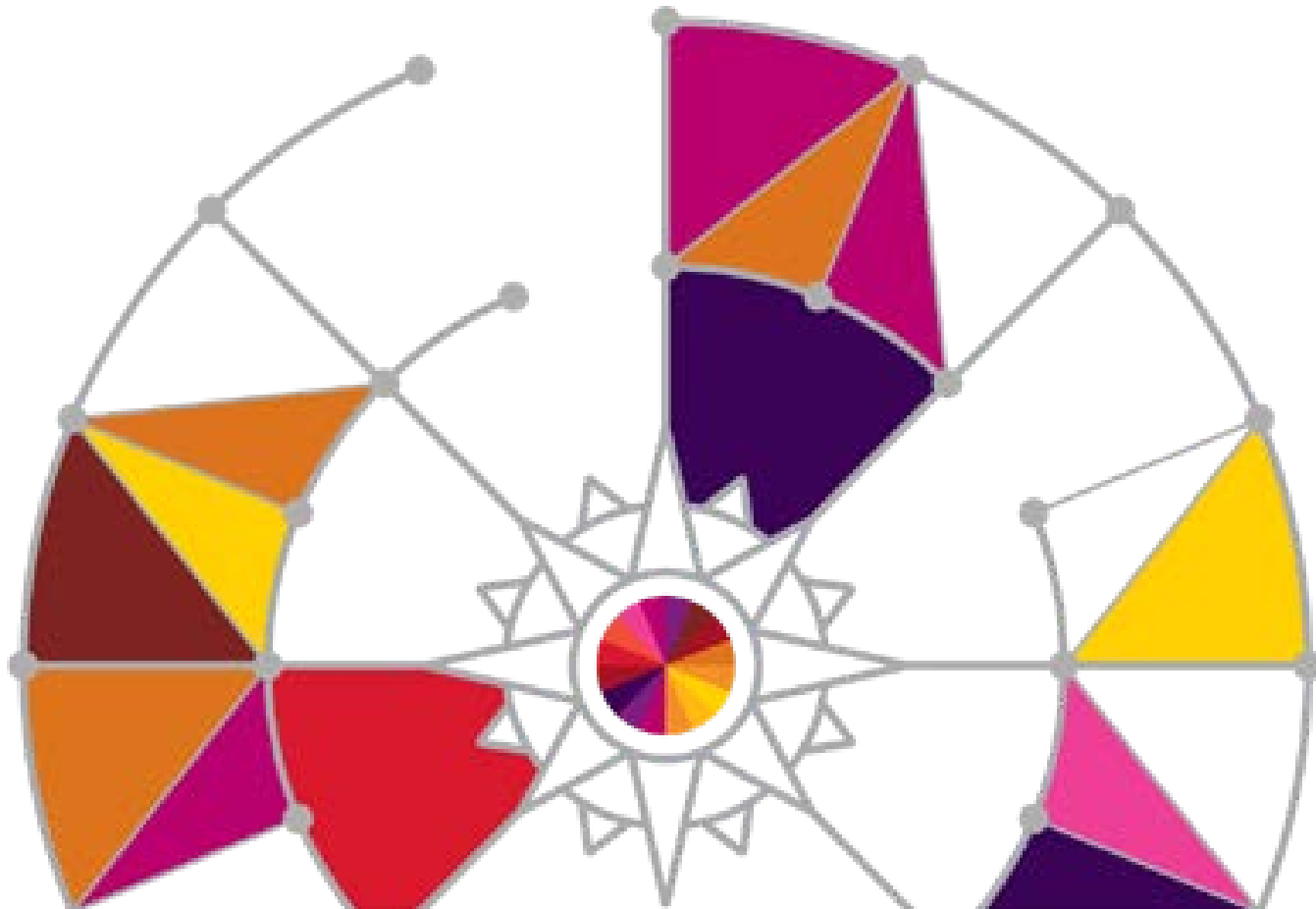
- ### Virtualization with partitions
- ### Cryptography
- zEnterprise 196 & zEnterprise 114
 - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions
 - System zEC12
 - Common Criteria EAL5+ with specific target of evaluation -- LPAR: Logical partitions
 - Crypto Express2 Coprocessor, Crypto Express3 & Crypto Express4s
 - FIPS 140-2 level 4 Hardware Evaluation
 - Approved by German ZKA
 - CP Assist
 - FIPS 197 (AES)
 - FIPS 46-3 (TDES)
 - FIPS 180-3 (Secure Hash)

IBM Solutions Help to Address Potential Security and Audit Concerns for the Mainframe



It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Questions any one?



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



ibm.com/security

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.