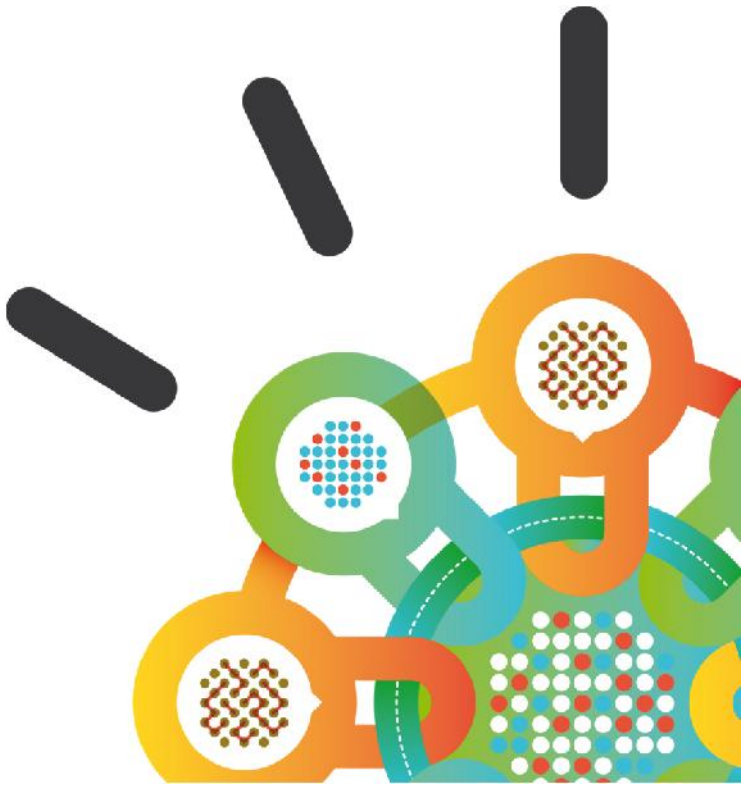
Security Intelligence.
Think Integrated.

How to take the complexity out of compliance

October 2014

Glinda Cummings CISA, CISSP
WW zSecure Product Manager



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 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.

Workloads that run on the Mainframe (System z)

What is a workload?

*The relationship between a **group** of applications and/or systems that are related across several business functions to satisfy one or more business processes, typically running on 'virtual servers'.*

Banking	Insurance	Retail	Healthcare	Public Sector
Core Banking	***Internet Rate Quotes***	***On-line Catalog***	***Patient Care Systems***	***Electronic IRS***
Wholesale Banking – Payments	***Policy Sales & Management (e.g. Life, Annuity, Auto)***	***Supply Chain Management***	***On– line Claims Submission & Payments***	***Web based Social Security***
Customer Care & Insight	***Claims Processing***	***Customer Analysis***		***Tax processing***

IBM's System z is Highly Securable

- Highly securable platform for virtual environments and workloads
  - **80%** of all active code runs on the Mainframe[1]
  - **80%** of enterprise business data is housed on the Mainframe[1]
  - ***This makes the Mainframe a desirable target for hackers***
- Security is built into every level of the System z structure
  - Processor
  - Hypervisor
  - Operating system
  - Communications
  - Storage
  - Applications
- System z security features address compliance
  - Identity and access management
  - Hardware and software encryption
  - Communication security capabilities
  - Extensive logging and reporting of security events
- Extensive security certifications (e.g., Common Criteria and FIPS 140) including EAL5+
- But today's mainframe must interoperate in a complex environment including cloud, mobile, big data and social networking and is susceptible to multiple vulnerabilities
  - [1]Source: 2013 IBM zEnterprise Technology Summit

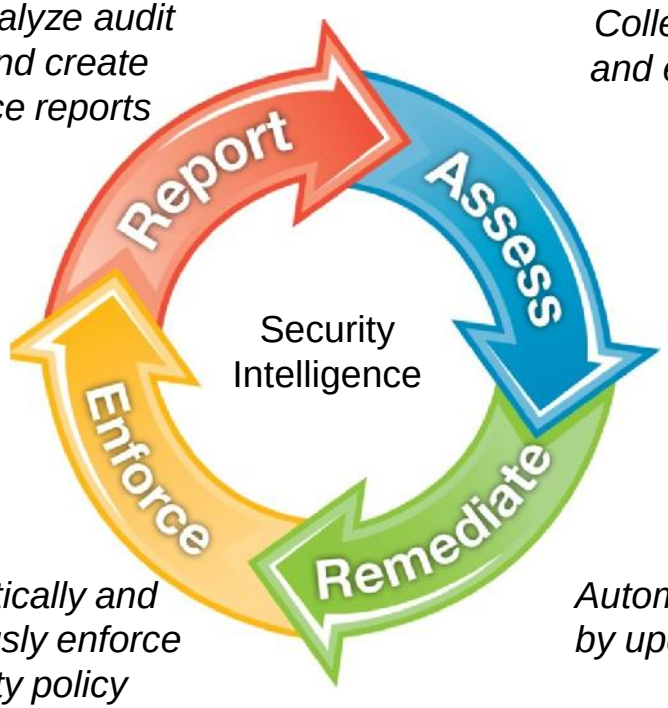
Common z/OS Security Challenges

- Legacy platform with legacy applications, legacy technicians
- Too many users with the ability to circumvent controls
- Inadequate attention to Reporting, let alone Monitoring, Alerting
- z/OS Unix managed by z/OS sysprogs
- Excessive access to utilities that allow bypassing of security policies
- Lax access controls allowing users to elevate privileges
- Poor data management practices for data access, copying & reuse
- Shared data between environments: development, test & production
- System z isolation – siloed from enterprise security monitoring
- Security architecture extensions for cloud, mobile, big data
- Insiders pose the greatest threat – insufficient detective controls
- Outdated security policy – does not meet modern standards

Security is a process

Monitor, analyze audit records and create compliance reports

Collect information, assess, and establish security policy



Automatically and continuously enforce security policy

Automate corrective actions by updating access controls

IBM Security zSecure Compliance and Admin

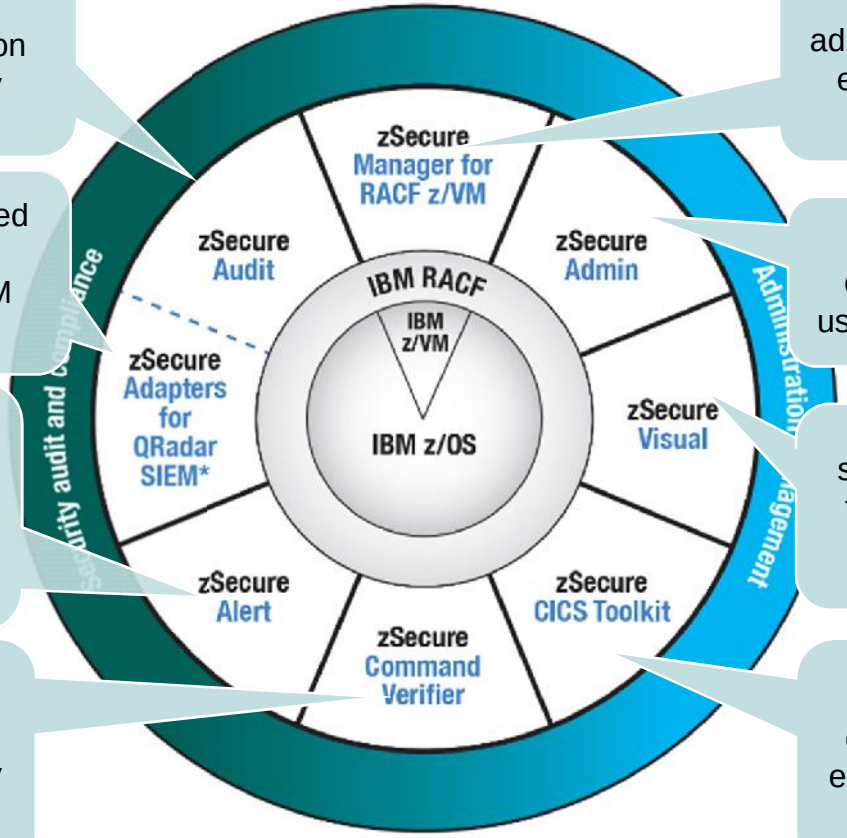
IBM Security zSecure helps address mainframe security challenges

Vulnerability analysis for the mainframe infrastructure. Automatically analyze and report on security events & detect security exposures

Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to IBM Security QRadar SIEM

Real-time mainframe threat monitoring permits you to monitor intruders and identify misconfigurations that could hamper your compliance efforts

Policy enforcement solution that helps enforce compliance to company and regulatory policies by preventing erroneous commands



Product offers a subset of the capabilities provided by zSecure Audit

Combined audit and administration for RACF in the VM environment including auditing Linux on System z

Enables more efficient and effective RACF administration, using significantly fewer resources

Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Provides access RACF command & APIs from a CICS environment, allowing additional administrative flexibility

Older zSecure versions – drawbacks with compliance testing

- Builtin standards (C1 / C2 / B1) were inflexible
  - Need to adapt more quickly to external standard updates
  - Audit concern principle misses the positive confirmation that it is OK
  - Audit concerns not customizable (exceptions / mitigating controls)
- Customers created ad-hoc reporting, partly 2-pass queries
  - Need something less ad-hoc and easier to customize
  - Need something that works almost out of the box
  - Need to combine information from many report types
  - Need to customize / define who is considered authorized
- Scope of external standards is increasing
  - Need to collect more settings from more subsystems.

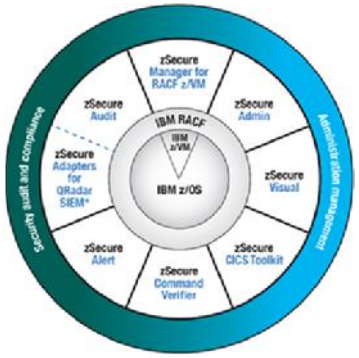
More flexibility please! The zSecure Compliance Testing Framework

- Support newer external standards
  - DISA STIG for z/OS RACF
  - DISA STIG for z/OS ACF2
  - PCI DSS
  - IBM outsourcing GSD331/iSec
- Eliminate need for 2-pass queries
- Show positive compliance, not just non-compliance
- Summaries showing progress in compliance efforts
- Support in-standard customization
  - Members with authorized (compliant) IDs (using STIG naming)
  - Allow rule override (suppression) with reason – visible in reporting
  - Allow creation and seamless integration of site standards
- Extend data collection CICS, IMS, DB2, MQ, IP, FTP, TELNET, some UNIX

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

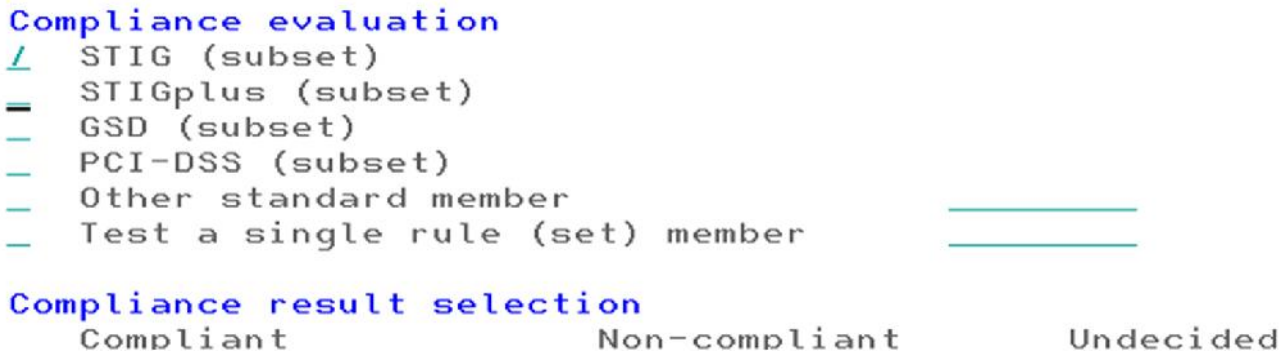
** GSD331: IBM's primary information security controls documentation for Strategic Outsourcing customers

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



Compliance reporting – Simple user interface

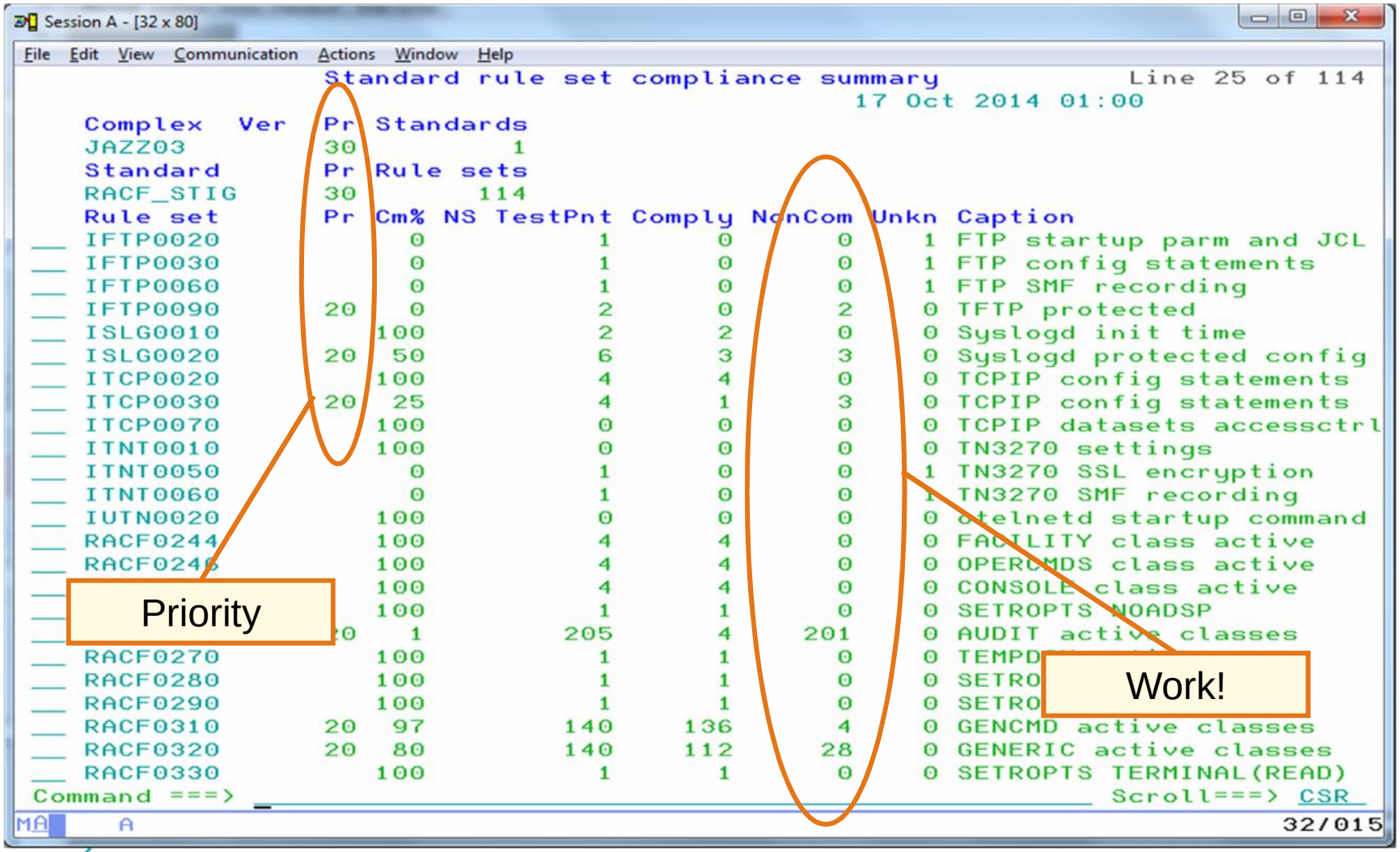
- Available in menu option AU.R



- run all available STIG rules/tests
- run all available GSD331 rules/tests
- run all available PCI-DSS rules/tests
- run individual rule

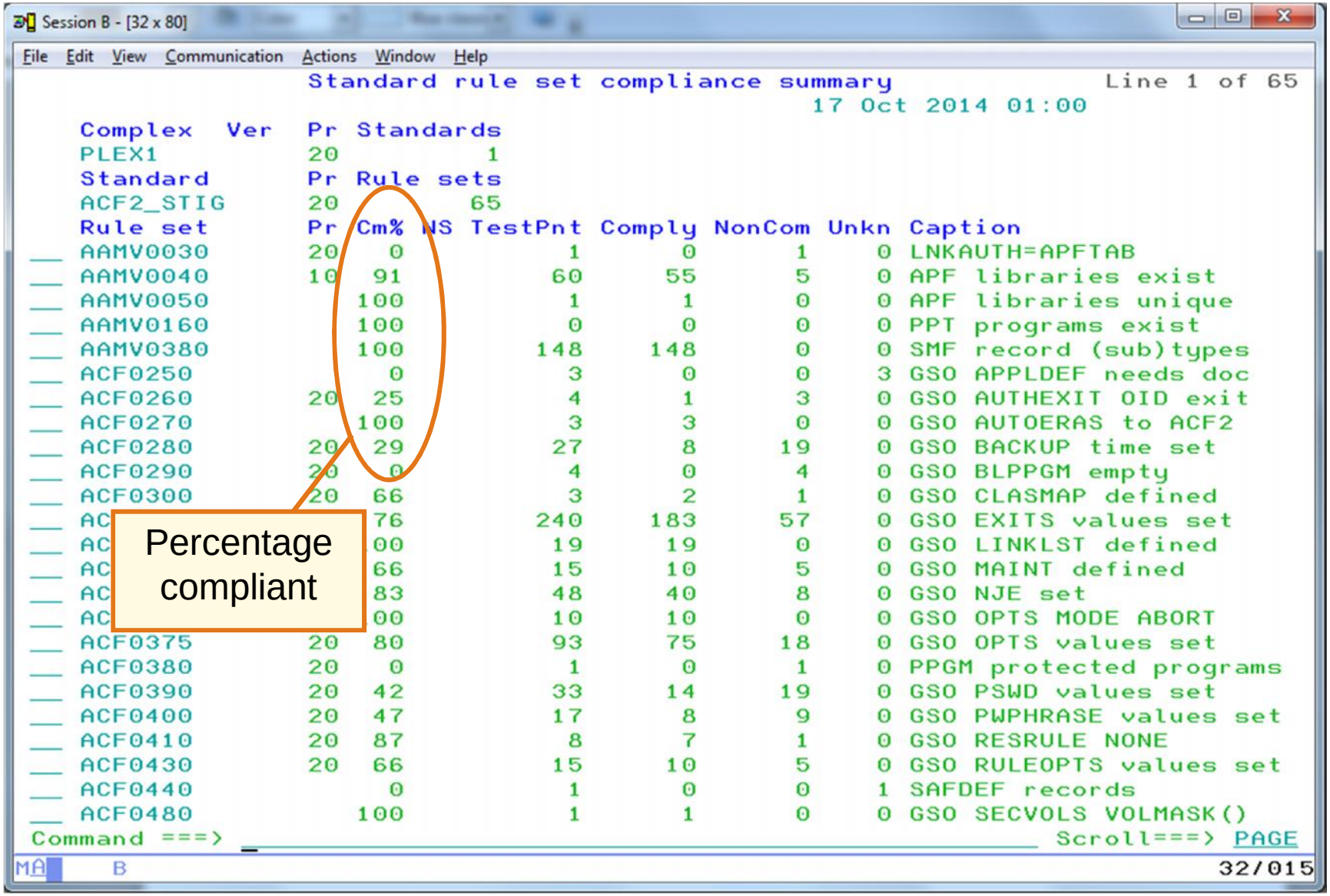
Choose results to include in report (none=all)

Compliance reporting – Sample output RACF



- ✓ RULE_SET names and percentage compliant state

Compliance reporting – Sample output ACF2



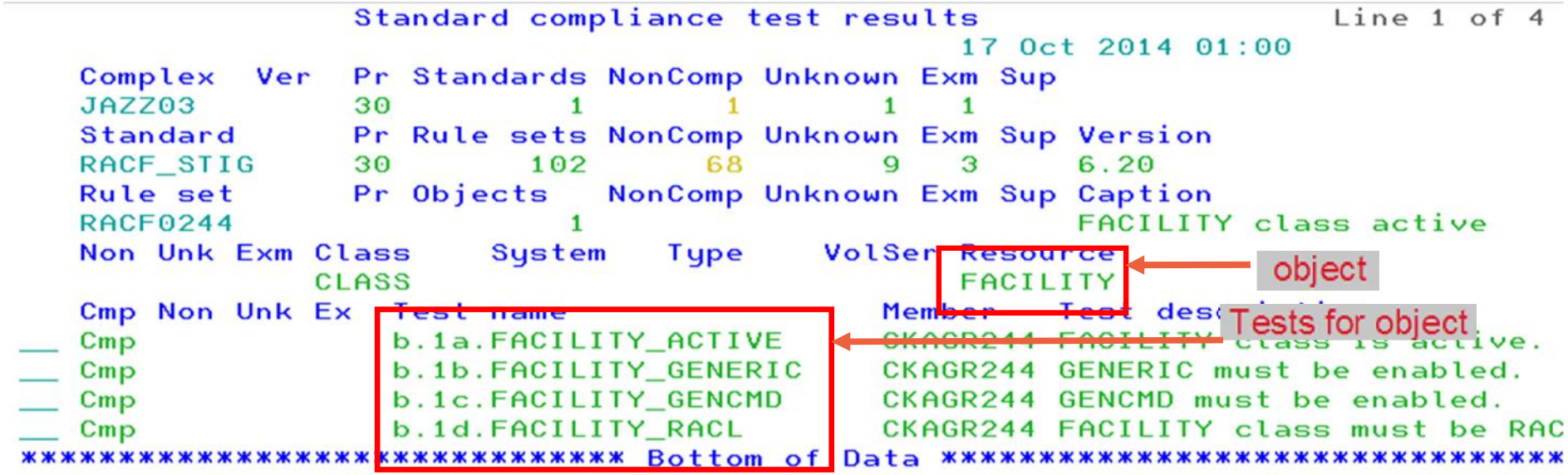
Session B - [32 x 80]

File Edit View Communication Actions Window Help

```
                    Standard rule set compliance summary              Line 1 of 65
                                                          17 Oct 2014 01:00
    Complex   Ver   Pr Standards
    PLEX1           20          1
    Standard        Pr Rule sets
    ACF2_STIG       20         65
    Rule set        Pr Cm% NS TestPnt Comply NonCom Unkn Caption
___ AAMV0030        20   0          1      0      1    0 LNKAUTH=APFTAB
___ AAMV0040        10  91         60     55      5    0 APF libraries exist
___ AAMV0050           100          1      1      0    0 APF libraries unique
___ AAMV0160           100          0      0      0    0 PPT programs exist
___ AAMV0380           100        148    148      0    0 SMF record (sub)types
___ ACF0250              0          3      0      0    3 GSO APPLDEF needs doc
___ ACF0260        20   25          4      1      3    0 GSO AUTHEXIT OID exit
___ ACF0270           100          3      3      0    0 GSO AUTOERAS to ACF2
___ ACF0280        20   29         27      8     19    0 GSO BACKUP time set
___ ACF0290        20    0          4      0      4    0 GSO BLPPGM empty
___ ACF0300        20   66          3      2      1    0 GSO CLASMAP defined
___ AC                  76        240    183     57    0 GSO EXITS values set
___ AC                  00         19     19      0    0 GSO LINKLST defined
___ AC                  66         15     10      5    0 GSO MAINT defined
___ AC                  83         48     40      8    0 GSO NJE set
___ AC                  00         10     10      0    0 GSO OPTS MODE ABORT
___ ACF0375        20   80         93     75     18    0 GSO OPTS values set
___ ACF0380        20    0          1      0      1    0 PPGM protected programs
___ ACF0390        20   42         33     14     19    0 GSO PSWD values set
___ ACF0400        20   47         17      8      9    0 GSO PWPHRASE values set
___ ACF0410        20   87          8      7      1    0 GSO RESRULE NONE
___ ACF0430        20   66         15     10      5    0 GSO RULEOPTS values set
___ ACF0440              0          1      0      0    1 SAFDEF records
___ ACF0480           100          1      1      0    0 GSO SECVOLS VOLMASK()
Command ===>                                              Scroll===> PAGE
MA      B                                                          32/015
```

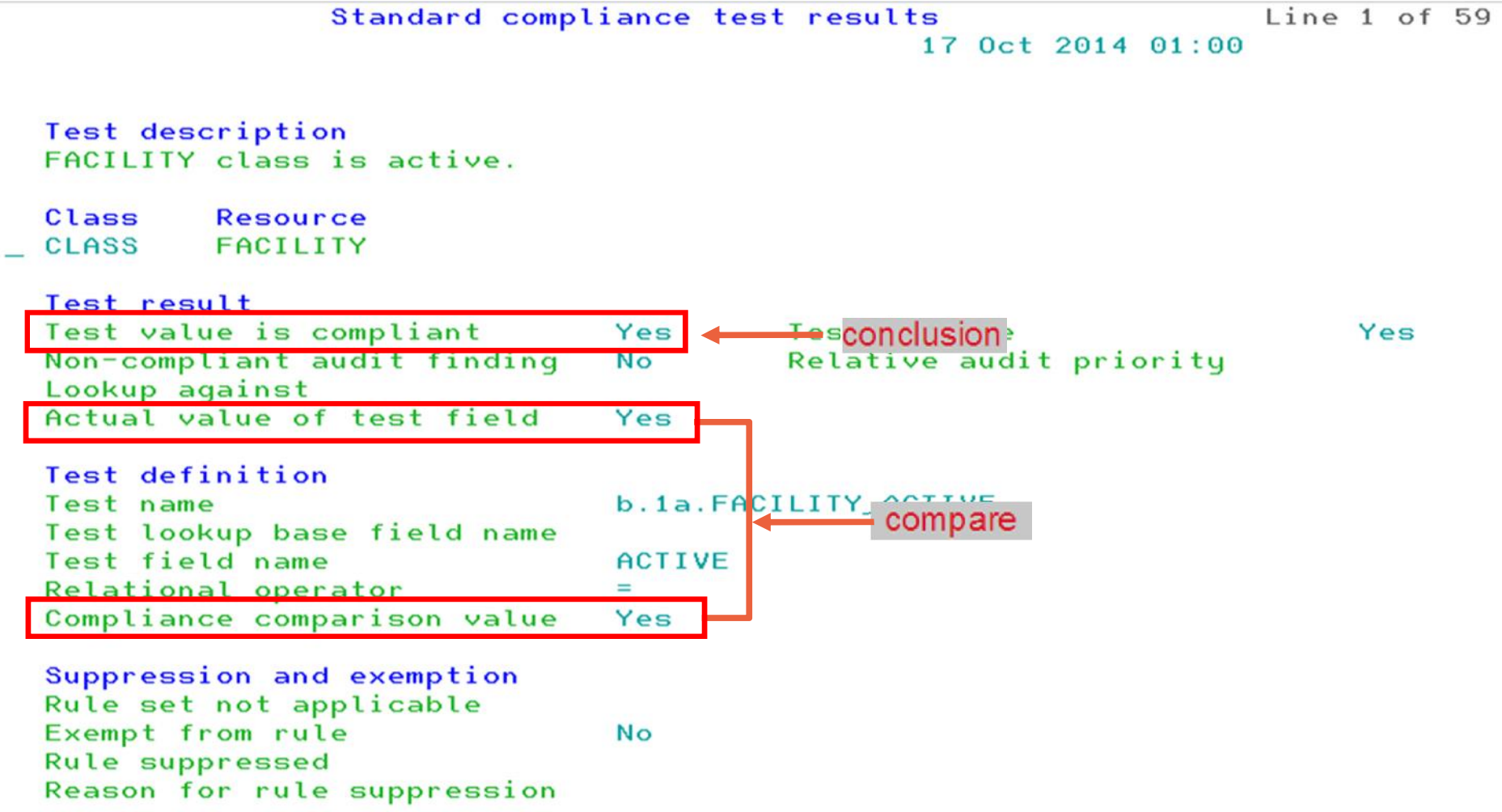
Percentage compliant

Compliance reporting – Zoom in to test level



✓Test names contain clear test numbers

Compliance reporting – Zoom in to detail level



Compliance reporting – detail level

- Scroll down to see

```
                  Standard compliance test results                Line 27 of 59
                                                    17 Oct 2014 01:00

  Domain
  Domain name                       FACILITY_class
  Domain description

  Rule
  Rule set                          RACF0244
  Rule name                         RACF0244
  Rule non-compliance severity      Medium    Site overruling rule severity

  Rule description
  FACILITY resource class must be active.

  Rule set description
  FACILITY resource class must be active.

  Standard
  Standard name                     RACF_STIG
  Version of standard               6.20



  Test origin
  Test defined in CARLa member      CKAGR244
********************************* Bottom of Data ********************************
Command ===>                                                 Scroll===> CSR
MA    A                                                              32/015
```

PCI-DSS rule set example

```
                    Standard rule set compliance summary              Line 1 of 13
                                                        17 Oct 2014 01:00
   Complex  Ver   Pr Standards
   JAZZ03           20          1
   Standard         Pr Rule sets
   RACF-PCI-DSS     20         13
   Rule set         Pr  Cm% NS TestPnt Comply NonCom Unkn Caption
__ 1.2.1            20    0           2      0      2    0 Restrict network traffic
__ 2.2.2                  0           1      0      0    1 Insecure services
__ 7.1.1            20    1          93      1     92    0 ID<>OWNER ALTER profiles
__ 7.2.3            20   95        4293   4097    196    0 Default deny all
__ 8.1              20   94         254    240     14    0 Unique user id
__ 8.4              20    0           3      0      2    1 Encrypt passwords
__ 8.5.5            20   50           2      1      1    0 SETROPTS INACTIVE(90)
__ 8.5.9            20   50           2      1      1    0 SETROPTS PASSW INT<=90
__ 8.5.10           20    0           1      0      1    0 SETROPTS PASSW LEN>=7
__ 8.5.12             100           1      1      0    0 SETROPTS PASSW HIST>=4
__ 8.5.13             100           2      2      0    0 SETROPTS PASSW REVOKE<=6
__ 10.2.2           20    2         350      7    343    0 Log root/admin actions
__ 10.2.5                 0           1      0      0    1 Log ident/authentication
****************************** Bottom of Data ******************************
```

Populate PCI-DSS definitions

- Data set with members to populate
  - New members for PCI-DSS:
    - CLASSIFY – Sensitive data sets
    - PCIAUTH – Users authorized for Authentication data
    - PCIPAN – Users authorized for Primary Account Numbers
    - PCIPANCL – Users authorized for Cleartext Primary Account Numbers

```
EDIT       IBMZSEC.DATA.SZT01.CKACUST(CLASSIFY) - 01.03    Columns 00001 00072
****** ***************************** Top of Data ******************************
000001  /* simulate commands for PCI-DSS data classification */
000002
000003 simulate class=dataset sensitivity=pci-pan resource=(,
000004 PAYROLL.EMPLOYEE.ADDRESS,
000005 PAYROLL.EMPLOYEE.SALARY,
000006 PAYROLL.EMPLOYEE.SERIAL,
000007 )
000008 simulate class=dataset sensitivity=pci-auth resource=(,
000009 IBMZSEC.DATA.FINANCE,
000010 )
****** ***************************** Bottom of Data ********************************
```

```
EDIT       IBMZSEC.DATA.SZT01.CKACUST(PCIAUTH) - 01.
****** ***************************** Top of Data ***
000001  /* users with access to resources containing
000002     sensitive authentication information */
000003 PCITEAM1
000004 PCIUSER1
****** ***************************** Bottom of Data *
```

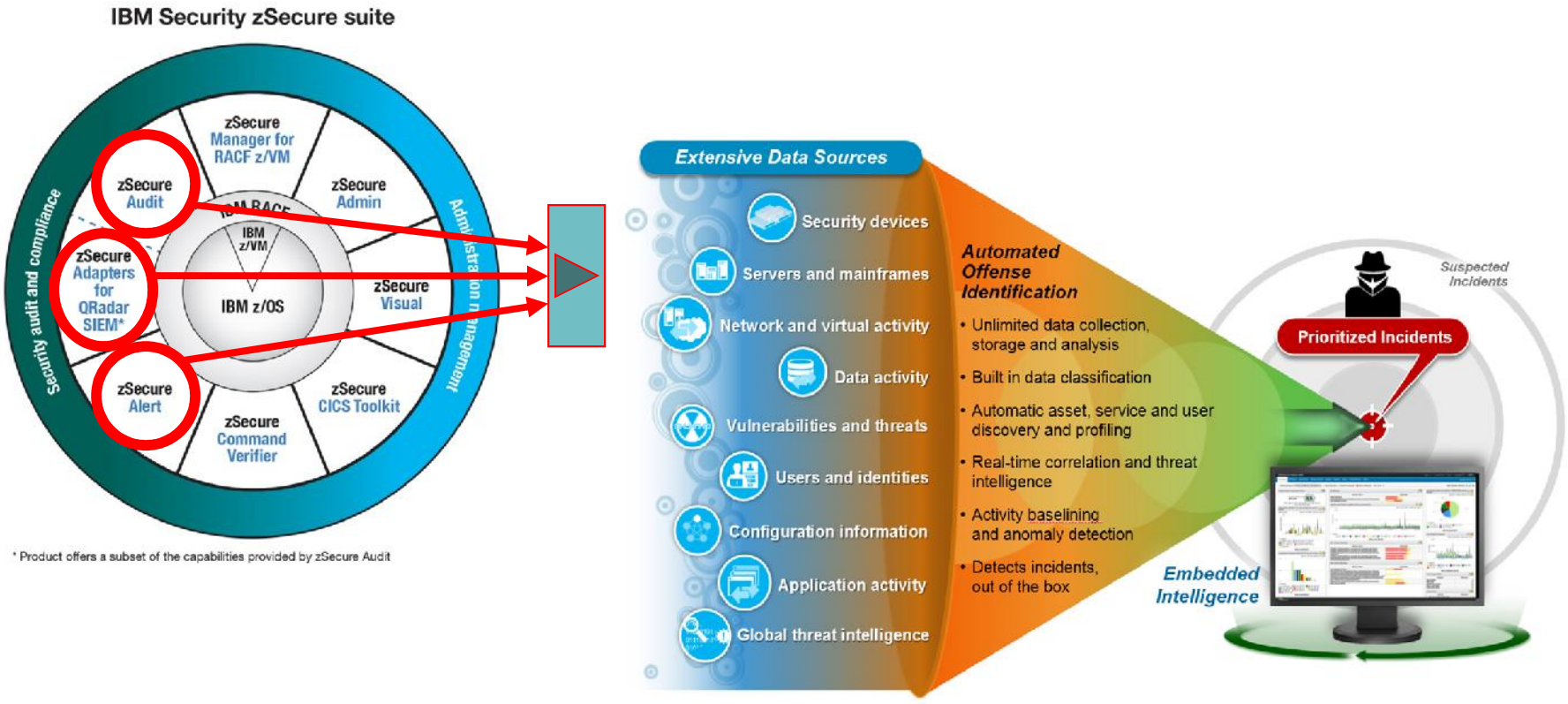
Gain a better understanding of your privileged user base

- Undoubtedly in the top 10 list of compliance failings . . . . too many privileged users!
- zSecure can tell you the access paths that can enable a user to bypass security

```
                                                                Line 19 of 521
Trusted userids (may bypass security)
                                                    17 Oct 2014 01:00
   Pri Complex  Trusted userids
    49 JAZZ03                521
   Pri Reasons Userid   Name                      RIP DfltGrp  InstData
__  10      614 U866ABC  DEX DEXTER 1                SYSPROG   GB061621 LONDON
__  10      611 U866ABC9 DEX DEXTER 9                SYSPROG   GB061621 LONDON
__  10      611 U866ACD  DEX DEXTER 11               U866      GB061621 LONDON
__  10      608 SYSPRG1  SYSTEM PRGM                 SYSPROG


    Pri Reasons Userid   Name                       RIP DfltGrp  InstData
     10      614 U866ABC  DEX DEXTER 1                SYSPROG   GB061621 LONDON
    Pri Cnt Audit concern
__   10   9 Can submit jobs for trusted user
__    9   1 Can (un)mount any HFS, honouring setuid and APF bits
__    9   1 Can make HFS file APF-authorized, APF program can bypass security
__    9   1 May change APF REXX that can bypass security
__    9   1 Systemwide authority to process data sets
__    9   1 User privileges and rules may be changed directly on disk
__    9   3 Security-relevant parameters may be changed
__    9   5 JCL that runs with high authority may be changed
__    9 150 May change APF program that can bypass security
      8   1 Can alter the RMM control data set, thus gaining access to any tape.
```

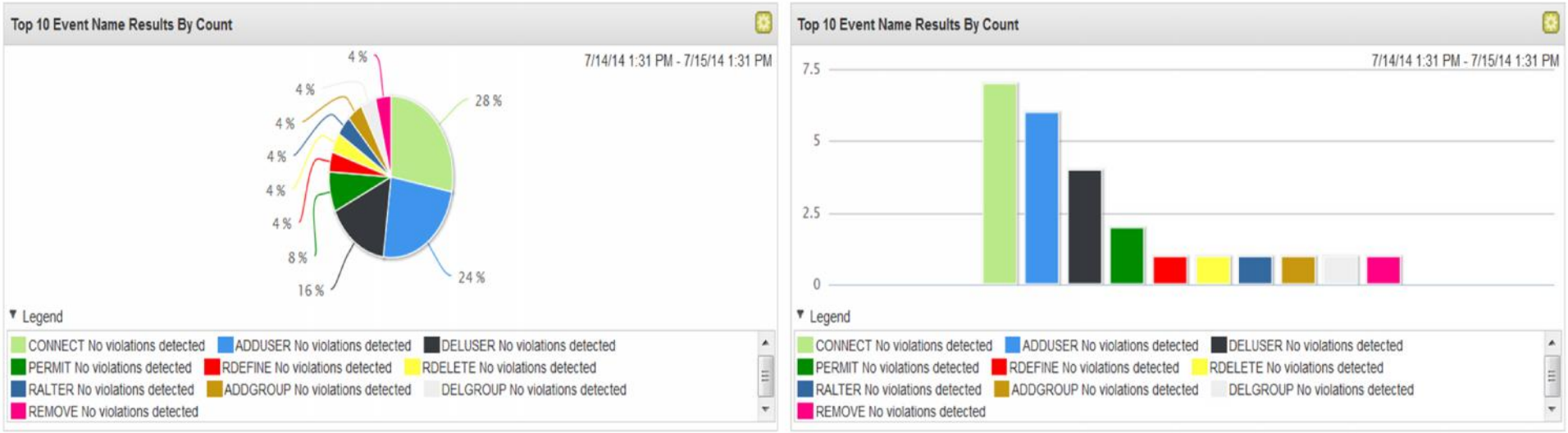
Security Monitoring - zSecure integration with QRadar SIEM



Event sources from System z . . .

z/OS	RACF	CA ACF2	CA Top Secret	CICS	DB2

Use QRadar to monitor security events from System z



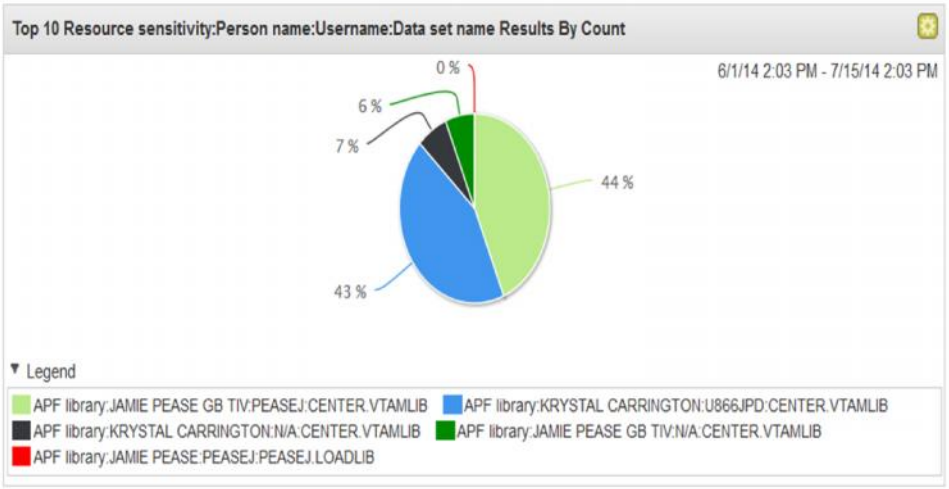
(Hide Charts)

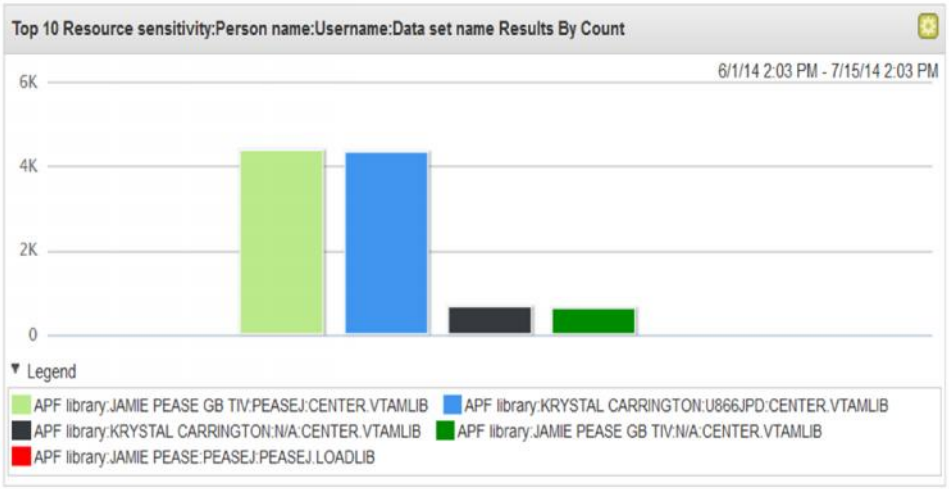
Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count
CONNECT No violations det...	Multiple (4)	7/14/14, 5:48:04 PM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success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

zSecure integration with QRadar can be used to monitor user behaviour - verify if users are complying with policy and standards

Event data collected by **zSecure Audit**

Using QRadar to monitor those privileged users on your mainframe





(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

QRadar Drilling into events collected from the mainframe

Resource sensitivity (custom)	APF library
SAF Class (custom)	DATASET
SAF resource name (custom)	PEASEJ.LOADLIB
SNA terminal name (custom)	ISZ004
Sensitive groups (custom)	N/A
Sensitive user privileges (custom)	special auditor
Submitted by (custom)	N/A
System SMF id (custom)	ZT01
System/job (custom)	ZT01 2 Jul 2014 08:07:42.72 PEASEJ
UNIX access origin (custom)	N/A
UNIX function (custom)	N/A
UNIX path name (custom)	N/A
Unix ACL group (custom)	N/A
Unix ACL type (custom)	N/A
Unix ACL user (custom)	N/A
Volume serial (custom)	*SMS*

Drill down

Source and Destination Information

Source IP	9.212.143.76

React quickly to non-compliant changes with zSecure Alert

- You need to be told immediately when changes occur that could create a compliance headache for you later!
- Suppose a compliance test was due the next day, however you were unaware that some non-compliant changes had just been implemented
- Finding out about such an event 24+ hours is no longer acceptable – the window of opportunity is too great.

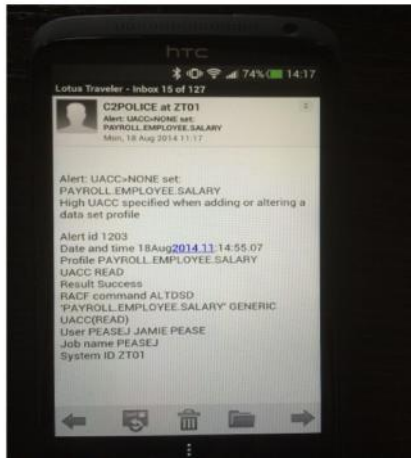
Alert: UACC>NONE set: PAYROLL.EMPLOYEE.SALARY

C2POLICE at ZT01 to: Jamie Pease, rob.vanhoboken, milos.kaljevic

Please respond to DontReply

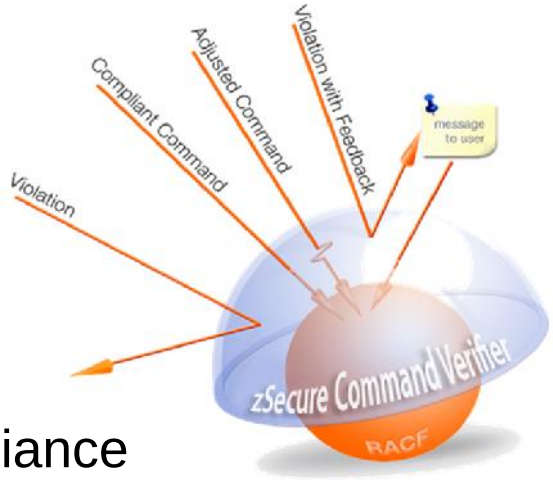
```
Alert: UACC>NONE set: PAYROLL.EMPLOYEE.SALARY
High UACC specified when adding or altering a data set profile

   Alert id          1203
   Date and time     18Aug2014 11:14:55.07
   Profile           PAYROLL.EMPLOYEE.SALARY
   UACC              READ
   Result            Success
   RACF command      ALTDSD 'PAYROLL.EMPLOYEE.SALARY' GENERIC UACC(READ)
   User              PEASEJ   JAMIE PEASE
   Job name          PEASEJ
   System ID         ZT01
```



Maintain compliance – prevent inappropriate changes

- People who implement security changes on System z can create "compliance issues"
  - These can occur for a number of reasons . . .
    - Not following standards, process . . .
    - Incorrect approval from an owner / authorizer
    - Lack of understanding
    - Failure to check and double check proposed changes



- zSecure Command Verifier can help maintain compliance

```
altdsd 'PAYROLL.EMPLOYEE.SALARY' generic  uacc(READ)
C4R646E Management of locked profiles not allowed, command terminated
```

```
SETROPTS  nosaudit
C4R751E SETROPTS SAUDIT not allowed, command terminated
```

```
connect (PEASEJ) group(PAYROLL) authority(USE) uacc(NONE)
C4R548E You may not connect yourself to group PAYROLL, command terminated
```


```
ralter STARTED C2ECQRLF.* STDATA(privileged(YES))
C4R716E Not allowed to set PRIVILEGED for STARTED profile
```

Compliance issues – perhaps your RACF database needs a cleanup

- Compliance issues (but not limited) to . . .
  - Unused user IDs
  - Excessive access
  - Inadequate reviews of access usage
- These can normally be addressed by a clean-up of your RACF database
- Customers often lack the technology to accurately collect “access usage”
- Clean up projects are often avoided or partially attempted due to incomplete data / too many unknowns
- Clean up should be continuous, not just a one time exercise
- **The solution: Access Monitor, part of zSecure Admin**

zSecure Admin - Access Monitor

Common Compliance Failure - Excessive Access!

- Part of your zSecure Admin license
- Use it for clean-up projects – the solution assists you with the following:-
  - Maintain an accurate record of “used” and “unused” access
  - Identify and remove unused access, such as access control list entries
  - Identify and remove unused group connects
  - Identify and remove unused profiles (including user IDs, dataset/general resource profiles)
  - Improve testing of security changes . . . simulate the effect of your proposed clean-up
  - Quickly back-out changes associated with RACF database clean-up
- Overall, helps to:
  - Remove excessive, unneeded access
  - Reduce risk and costs associated with clean-up projects
  - Simplify the implementation of Role Based Access Control initiatives
  - Improve RACF performance
  - Reduce audit concerns and comply with policy, standards and regulations

Security is a process, zSecure is the toolbox

zSecure Audit:
compliance reports

QRadar SIEM

zSecure Audit:
automated vulnerability finder

zSecure Audit reports

zSecure Alert

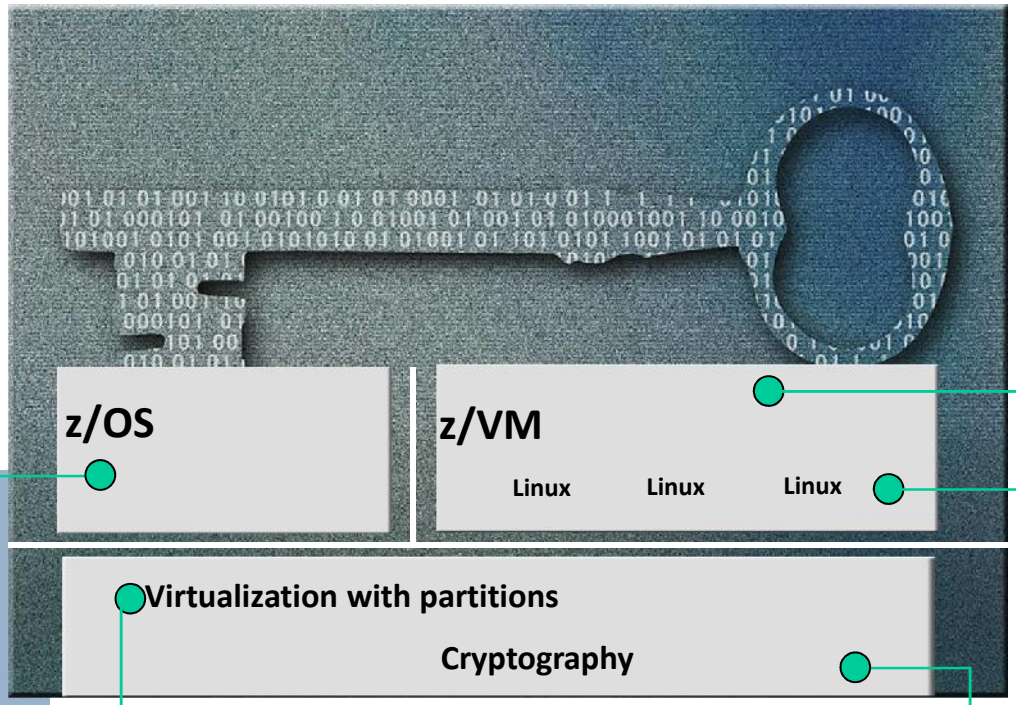
zSecure Command Verifier

zSecure Admin:
Access Monitor
RACF Offline

IBM Security zSecure Compliance and Admin

System z Certifications & Evaluations

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



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, z/OS V2.1 (OSPP)
- Common Criteria EAL5+
  - RACF V1R12, 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

z/VM

- Common Criteria
  - z/VM 6.1 is EAL 4+ for OSPP
- z/VM 6.3 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

- zEnterprise 196 & zEnterprise 114
  - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions
- System zEC12 & BC12
  - 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)

29

zSecure strategy

- The value of zSecure, its success and growth lies in its capability to meet current and emerging customer needs for System z security implementation integrity and assurance.
  - Highly integrated and in “lock step” with RACF, z/OS, z/OS subsystems, middleware and applications
- Customer needs are driven by the ever-evolving threats, innovative business processes, and services built on technology, extensions of System z capabilities, and relevant laws and regulations around the globe.
- zSecure strategy continues on the path of integration of auditing and alerting for System z, subsystems, products, and applications, delivery of customizable reporting and analysis of audit records, and enhanced threat monitoring.
  - Enhanced threat monitoring will focus on expanding access monitoring, and other monitoring functions within the zSecure suite. This also encompasses off-line analysis of the RACF database
  - Continued focus on integrity and security by providing integration with other IBM monitoring and security technology
- Addressing the need for simplification -- zSecure direction is to expand coverage of System z administration capabilities and ease of use.
- Recognizing that clients may use a variety of other security governance, risk, and compliance products -- identify and establish easy and high-value interfaces to enable System z integration with other solutions.

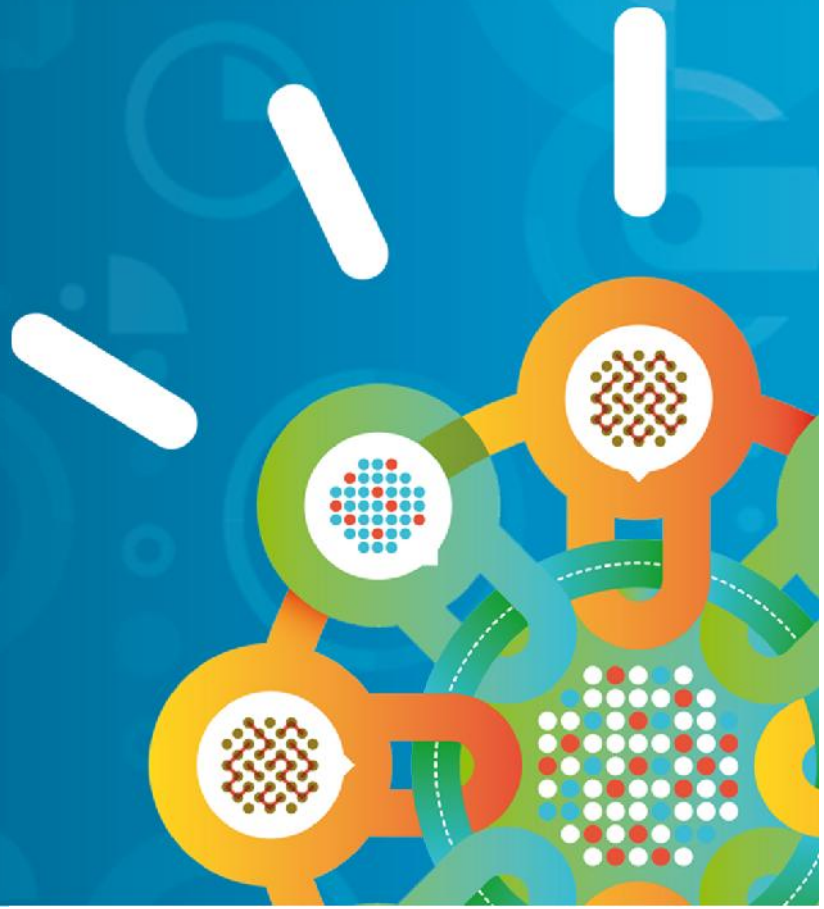
zSecure Products

- New releases for z/OS products
  - 5655-N16 IBM Security zSecure Admin 2.1.1
  - 5655-N20 IBM Security zSecure Visual 2.1.1
  - 5655-N17 IBM Security zSecure Audit 2.1.1
  - 5655-N21 IBM Security zSecure Alert 2.1.1
  - 5655-N19 IBM Security zSecure Command Verifier 2.1.1
  - 5655-N18 IBM Security zSecure CICS Toolkit 2.1.1
  - 5655-AD8 IBM Security zSecure Adapters for QRadar SIEM 2.1.1

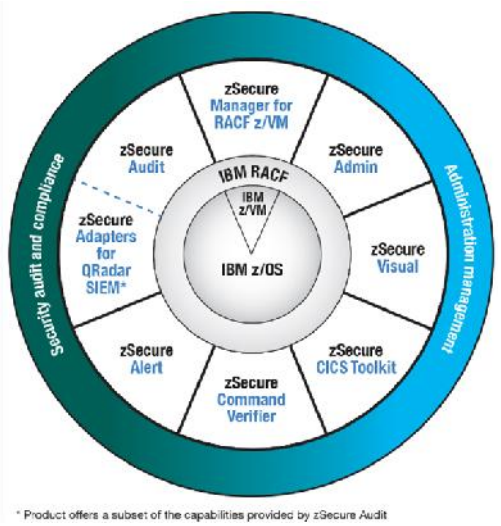
- z/VM offering
  - 5655-T13 IBM Security zSecure Manager for RACF z/VM

- zSecure solution sets
  - 5655-N25 IBM Security zSecure Compliance and Administration 2.1.1
  - 5655-N24 IBM Security zSecure Compliance and Auditing 2.1.1
  - 5655-N23 IBM Security zSecure Administration 2.1.1

Questions



zSecure suite Business Benefits



- Helps to reduce cost and improves resource utilization
  - Task automation reduces labor cost to perform essential z/OS and RACF security functions
  - Simplified UI allows less experienced resources to perform key security functions, freeing up skilled mainframe resources and allowing administer to manage security rather than using system programmer skills.
  - Improved system availability with automated analysis and detection of threats and configuration changes.
- Proactive compliance monitoring
  - Automated compliance monitoring, customized to fit your business, issues real time alerts on external threats, inappropriate data access or misconfiguration
  - Real-time blocking of dangerous RACF commands helps prevent privileged user abuse
  - Automated data collection for compliance reporting, audit trail analysis and forensic research.
  - Automated compliance testing framework
- Security Intelligence integration for enterprise-wide threat protection
- Improves efficiency and quality
  - Automated functions reduce mistakes that lead to data exposure and costly outages
  - Single point of administration easily manages large and small z/OS environments, and multiple RACF databases
  - Streamlined management of privileged users quickly identifies & removes unnecessary access to information

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