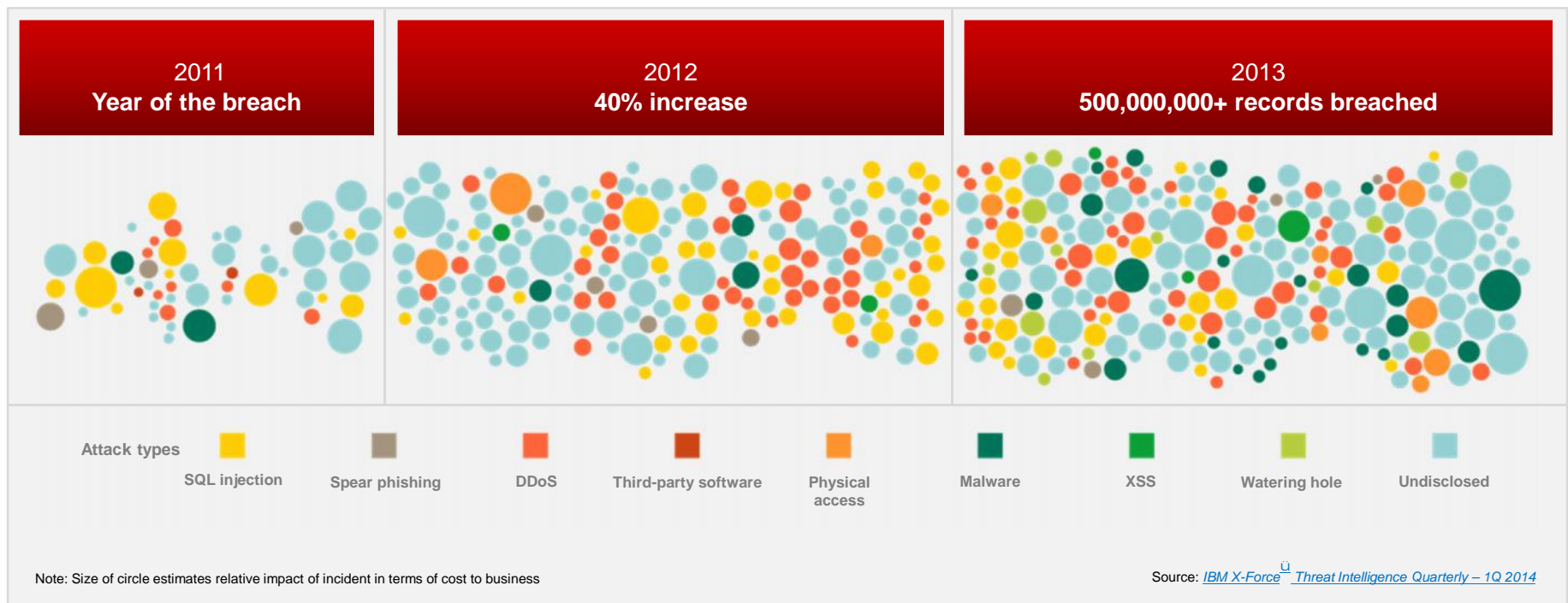




IBM z Systems – Compliance and Security Intelligence made easier



Sophisticated attackers break through safeguards every day



61% of organizations say **data theft and cybercrime** are their greatest threats

2012 IBM Global Reputational Risk & IT Study

\$3.5M⁺ average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

A new security reality is here

Sophisticated attackers break through conventional safeguards every day

61% of organizations say **data theft and cybercrime** are their greatest threats
2012 IBM Global Reputational Risk & IT Study

\$3.5M
 Average cost of a data breach
2014 Cost of Data Breach, Ponemon Institute

Cloud, mobile, social and big data drive unprecedented change

70% of security executives have **cloud and mobile security** concerns
2013 IBM CISO Survey

614%
 Mobile malware growth in just one year
2012 - 2013 Juniper Mobile Threat Report

Yesterday's security practices are unsustainable

83% of enterprises have difficulty finding the **security skills** they need
2012 ESG Research

85 security tools from **45** vendors
IBM client example

Security leaders are more accountable than ever before



Your board and CEO demand a strategy

As Cyber Attacks Detonate, Banks Gird For Battle

- Jamie Dimon, CEO, JPMorgan Chase & Co., acknowledged that attacks are becoming more complex and dangerous, no longer carried out by "fairly simplistic" hackers commandeering people's personal computers.
- "Now you're talking about state-sanctioned folks, hundreds of programmers," he said in a call with reporters this spring, "taking over not just PCs but servers and mainframes."(1)
- JPMorgan Chase & Co. is the largest bank in the United States second largest bank (2)



(1) <http://www.npr.org/templates/story/story.php?storyId=202645037>

(2) http://en.wikipedia.org/wiki/JPMorgan_Chase

The increasingly desirable target of the mainframe

80 % of all active code runs on the mainframe

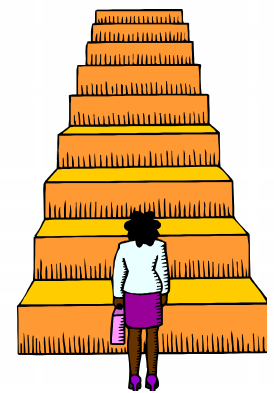
80 % of enterprise data is housed on the mainframe

Today's technologies have eliminated "mainframe isolation"



Security challenges specific to the mainframe

- Monitoring of security events from System z is often performed by the people that implement security changes!
 - Poor Separation of duties
 - Window of opportunity to commit fraud
 - Out dated practices
 - Staff unable to focus on improving security
- Silo approach . . . System z isolated from the Enterprise Security Monitoring practice
- Security Monitoring no longer fit for purpose, often running reports that were written 20 years ago . . . the threat and compliance landscape has changed significantly!
- Existing SIEM solution does not handle events from the mainframe very well
- Many events are not logged or reviewed
- Too many critical events are being reported 24+ hours later
- Security Monitoring does not meet compliance requirements



and more challenges

- The mainframe can be difficult to hack from the outside world, however it has been done!
- Biggest threat to the mainframe is the insider / internal attacks
 - Those employees with detailed knowledge of the systems – they also know how to circumvent controls
 - Many Security Monitoring implementations would not detect suspicious/inappropriate activities
 - Attackers can avoid detection for months/years



IBM z Systems are a highly securable environment

Security is embedded into the System z architecture

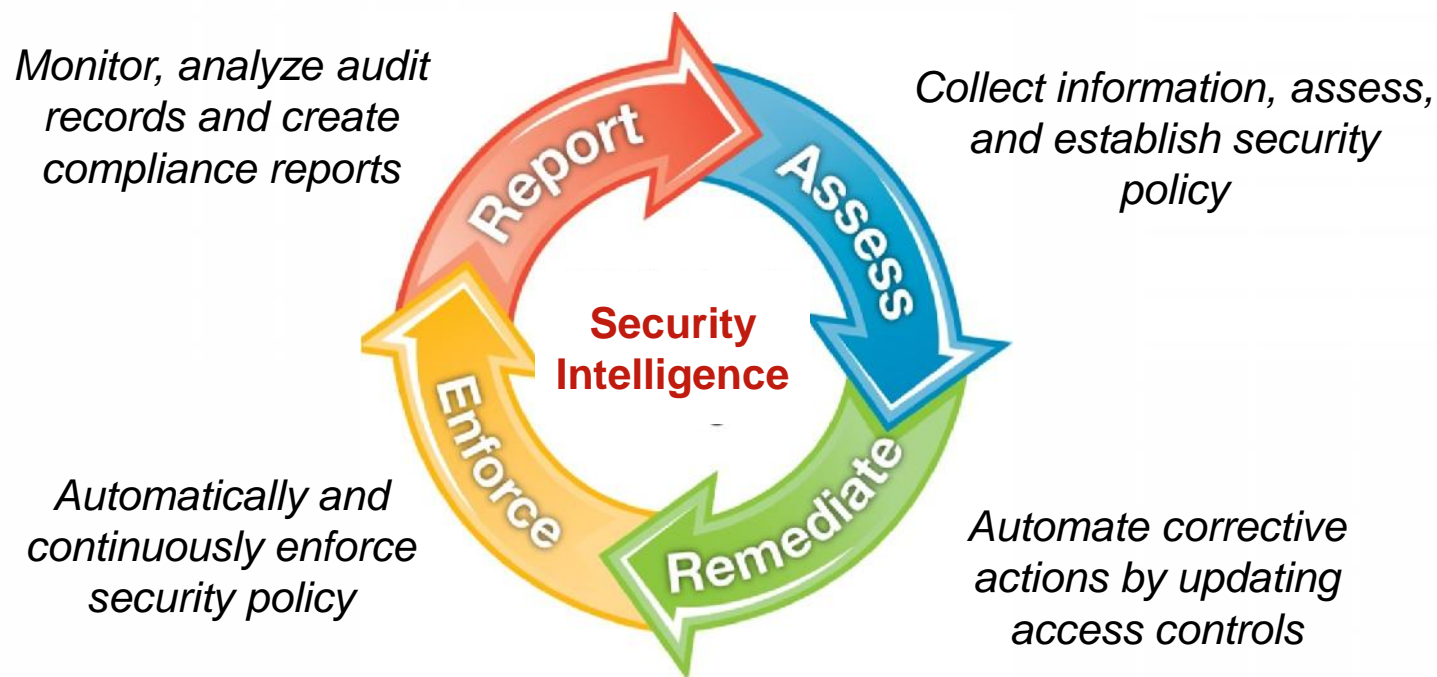
- Processor
- Hypervisor
- Operating system
- Communications
- Storage
- Applications



Z Systems security addresses regulatory compliance for:

- Identity and access management
- Hardware and software encryption
- Communication security capabilities
- Extensive security event logging and reporting capabilities
- Extensive security certifications including EAL5+ (e.g., *Common Criteria and FIPS 140*)

Customers need security intelligence: automated continuous compliance to address worldwide industry standards and regulations

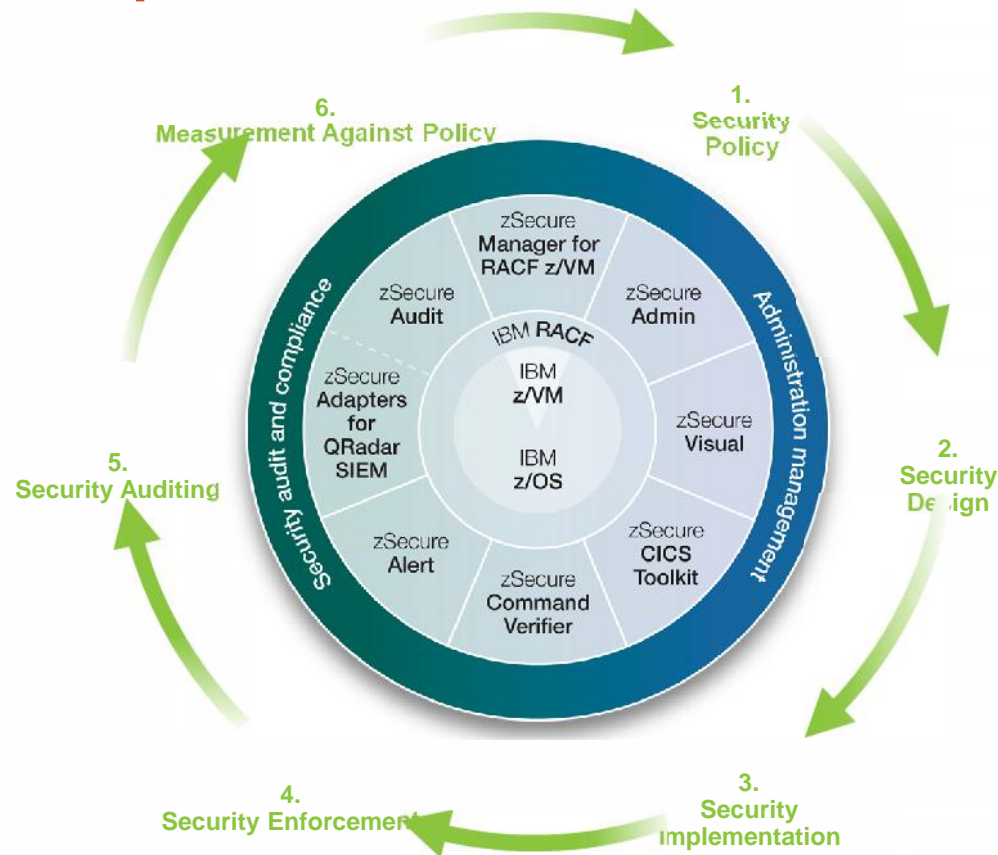


IBM Security zSecure Compliance and Audit



zSecure:

A comprehensive and continuous approach to mainframe security development





Addressing those challenges with IBM Security zSecure

zSecure Audit

Vulnerability analysis for the mainframe infrastructure; automatically analyze and report on security events and monitor compliance

zSecure Adapters for QRadar

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

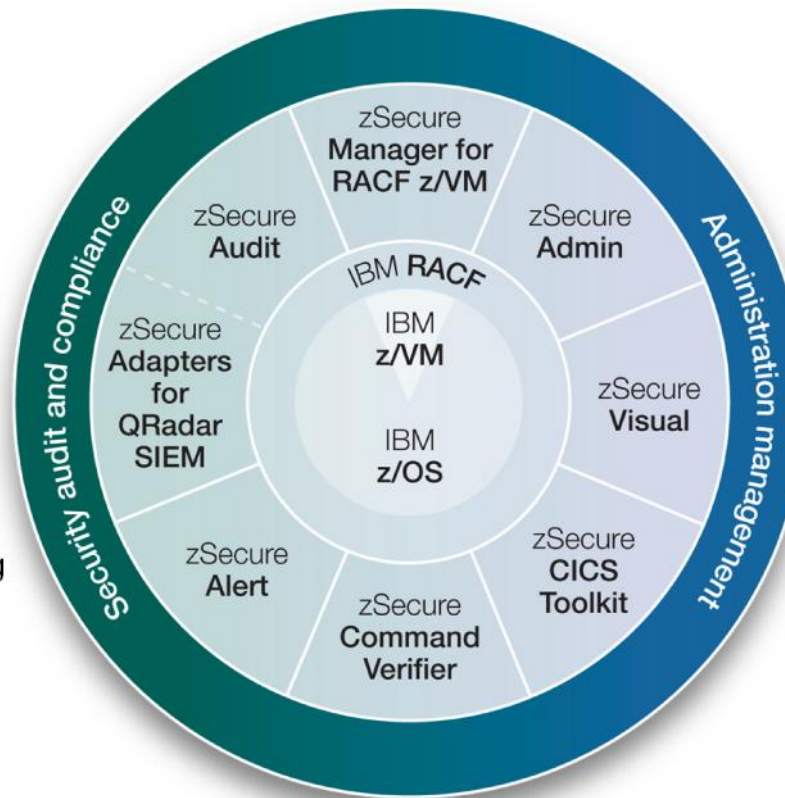
zSecure Alert

Real-time mainframe threat monitoring of intruders and alerting to identify misconfigurations that could hamper compliance

zSecure Command Verifier

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

IBM Security zSecure suite



Note:

- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

zSecure Manager for RACF z/VM

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

zSecure Admin

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

zSecure Visual

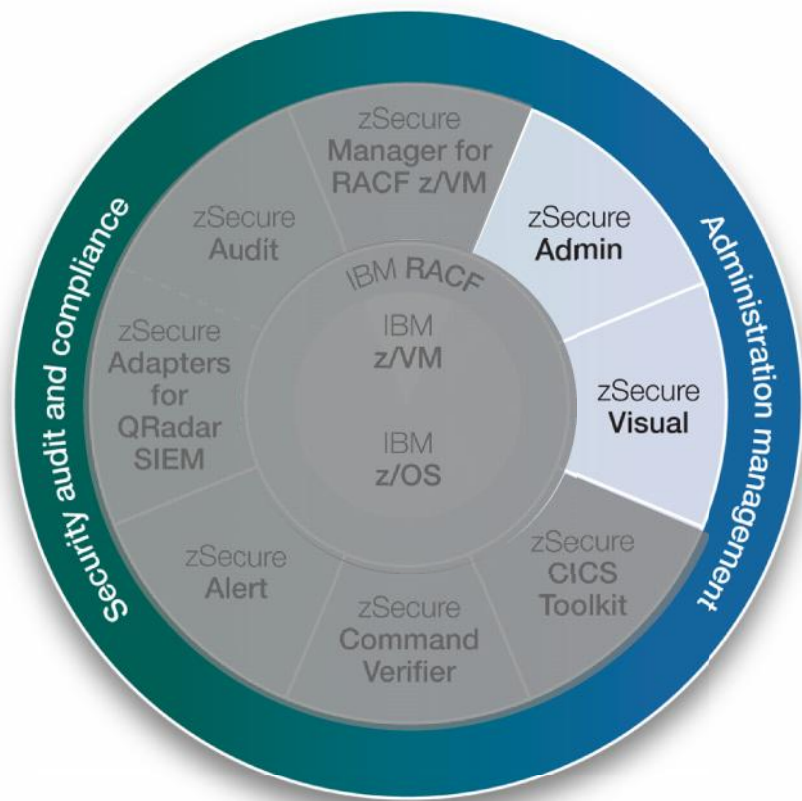
Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows-based GUI for RACF administration

zSecure CICS Toolkit

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

IBM Security zSecure Administration and Visual

IBM Security zSecure suite



Note:

- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

zSecure Admin

Improves the efficiency of admin and audit tasks with highly usable ISPF panels with overtyping capability

- Enables offline RACF database management and helps with merging RACF databases
- Provides access monitoring for RACF database cleanup and verifying validity of defined security
- Apply updates to multiple live RACF databases with or without RRSF from one single session
- Apply command to multiple profiles showing on a display
- Digital certificate administration with use case templates

zSecure Visual

Windows based GUI modernizes and helps with RACF consumability

- Specify once, execute on multiple systems
- Drag and drop administration

zSecure Admin - Access Monitor

Part of your zSecure Admin license

Common Compliance Failure - Excessive Access!

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

IBM Security zSecure Compliance and Auditing

zSecure Audit

Provides highly customizable reporting and analysis of audit records (SMF etc.)

- Includes events and compliance information from RACF, Top Secret, and ACF2 as well as subsystems such as DB2, CICS, IMS, MQ and more
- Reports on Compliance Framework for regulations including PCI-DSS, GSD331, and STIGS
- Collects, formats and sends enriched security information to QRadar SIEM for enterprise wide analysis and threat detection

zSecure Alert

Provides real time threat monitoring extending RACF and ACF2 real time notification capabilities

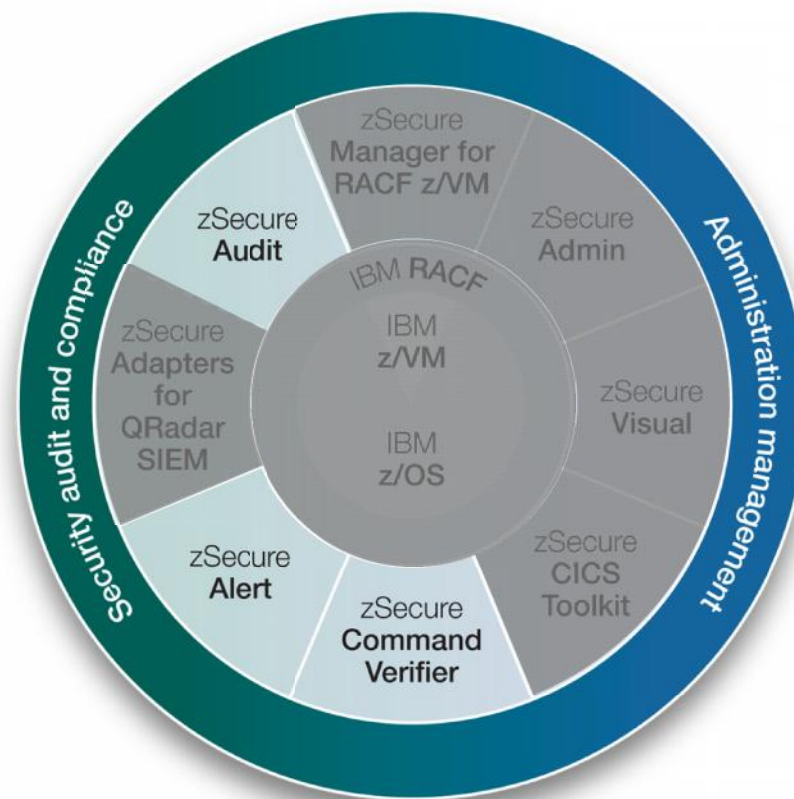
- Monitors for status changes in z/OS, RACF, and ACF2
- Alerts on PCI data

zSecure Command Verifier

Helps to control and maintain compliance by preventing RACF commands that are erroneous or do not adhere to corporate security policy

- Reduce database pollution by preventing noncompliant commands
- Reduce the risk of security breaches and failed audits caused by internal errors and noncompliant commands, enforce naming conventions

IBM Security zSecure suite



Note:

- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™



IBM Security zSecure suite automation capabilities

Security audit and compliance



Enhanced data collection z

of SMF audit information from:

- RACF, DB2, CICS, IMS, MQ, SKLM, WAS, UNIX, Linux on z Systems, OMEGAMON XE on z/OS, FTP, Communication Server, TCP/IP, PDSE and more

Automated remediation to detect and prioritize potential threats with security event analysis

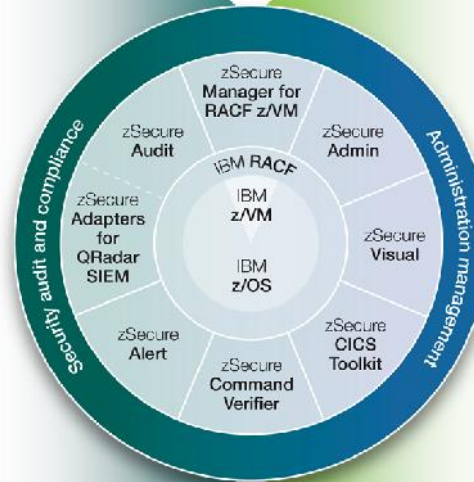
Real-time alerts of potential threats and vulnerabilities

Compliance monitoring and reporting

- PCI-DSS, STIGs, GSD331, and site-defined requirements

Comprehensive customized audit reporting

Detect harmful system security settings with automated configuration change checking



Administration management



Reduce administrative overhead with security management tasks

Prevent abuse of special roles and authorization with privileged user monitoring

Enforce security policies by blocking dangerous commands and potential errors

RACF data set cleanup of unused security profiles and inactive / terminated users



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

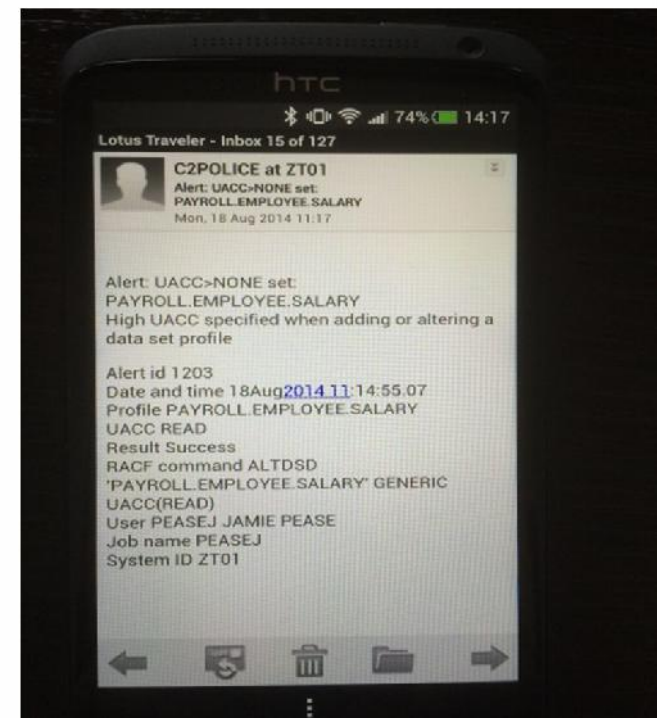
Finding out about such an event 24+ hours is no longer acceptable – the window of opportunity is too great.



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 ALTDSO 'PAYROLL.EMPLOYEE.SALARY' GENERIC UACC(READ)
User        PEASEJ  JAMIE PEASE
Job name    PEASEJ
System ID   ZT01
```



Security Assessment - 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

Benefits:

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



* 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

PCI-DSS rule set example

```

Standard compliance test results          2 s elapsed, 1.9 s CPU
Command ==> █                               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
***** Bottom of Data *****

```

Zoomable compliance test details

Standard compliance test results Line 1 of 92
 Command ==> Scroll==> CSR_
30 Jun 2014 07:46

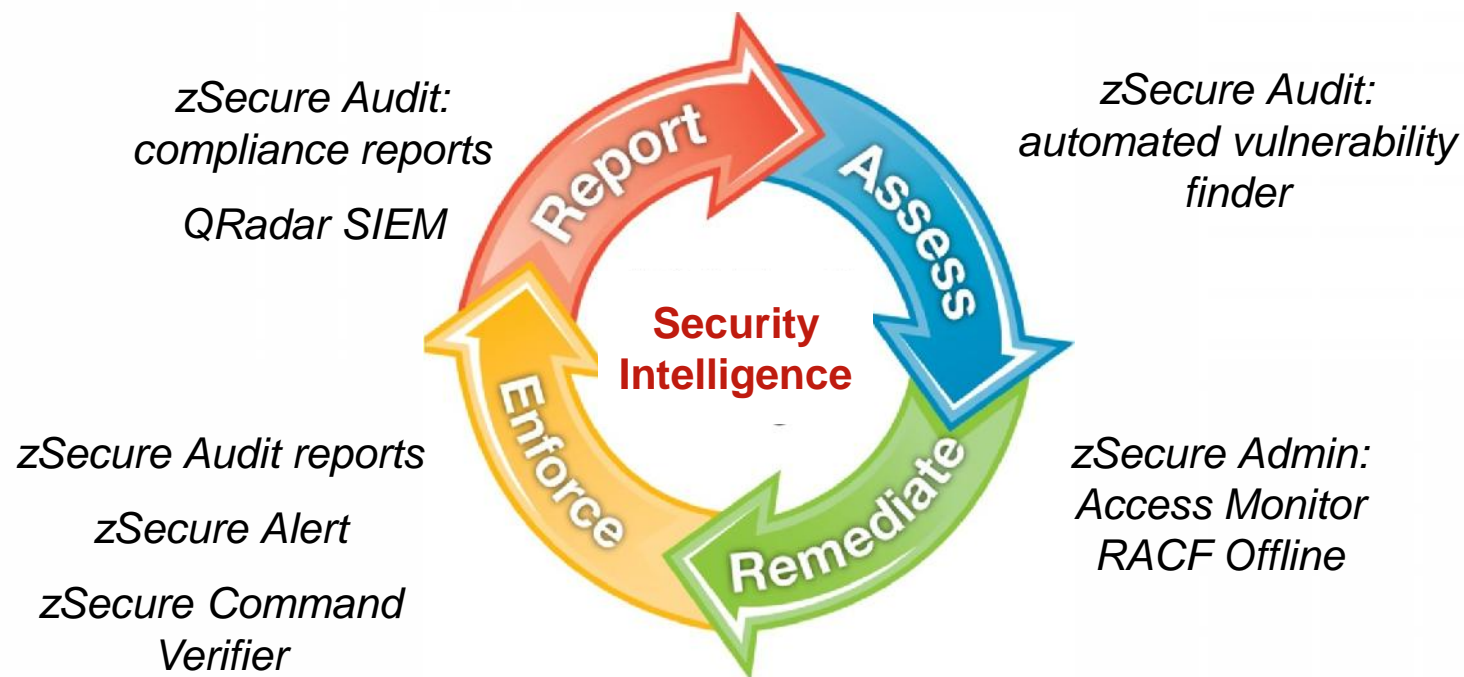
Complex	Ver	Pr	Standards	NonComp	Unknown	Exm	Sup	Version
NM87	NM87	30	1					
RACF_STIG		30	92	58	3	4		6-19
Rule set	Pr	Objects	NonComp	Unknown	Exm	Sup	Caption	
AAMV0030	20	1	1				LNKAUTH=APFTAB	
AAMV0040	10	630	101				APF libraries exist	
AAMV0050		14					APF libraries unique	
AAMV0160	20	132	26				PPT 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	
	30	5	4				RACF db protected	
	30	25	17				JES data sets protected	
ACP00170	30	9	8				UADS protected	
ACP00250	30	15	13				PROCLIBs protected	
ACP00260	20	2	2				FEABD profile protection	
ACP00350		1					Protection	
IFTP0020		1					ftp parm and JCL	
IFTP0030		1					FTP config statements	
IFTP0060		1					FTP SMF recording	
IFTP0090	20	1	1				TFTP protected	
ISLG0010		2					Syslogd init time	

Narrow captions

Priority

Work!

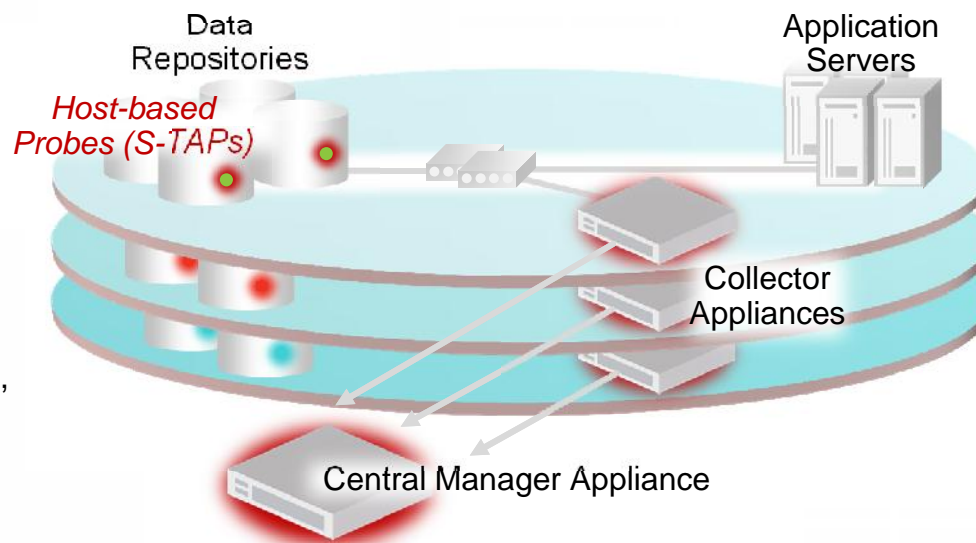
In summary: Security is a process, zSecure is the toolbox



IBM Security zSecure Compliance and Admin

IBM InfoSphere Guardium real-time activity monitoring

- Activity Monitoring**
 Continuous policy-based real-time monitoring of all data traffic activities, including actions by privileged users
- Blocking and Masking**
 Automated data protection compliance
- Vulnerability Assessment**
 Database infrastructure scanning for missing patches, misconfigured privileges, and other vulnerabilities

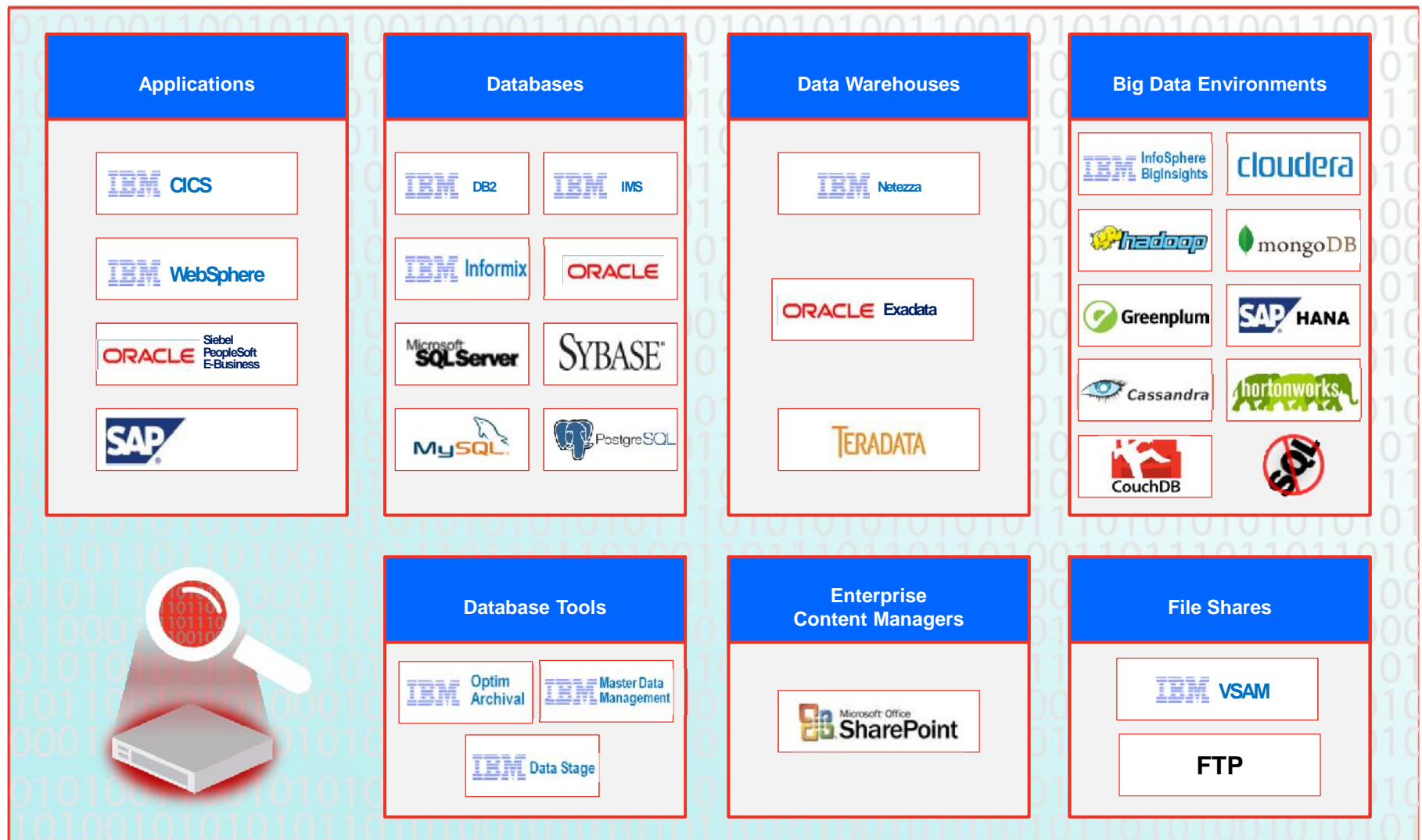


Key functionality

- Non-invasive / disruptive, cross-platform architecture
- Dynamically scalable
- Separation of Duties enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized and suspicious activity
- Granular, real-time policies (*who, what, when, how*)
- Doesn't rely on resident logs that are easily erased by attackers and rogue insiders
- No environment changes
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Real-time Data Activity Monitoring across the enterprise

For data warehouses, Big Data environments, and file shares



What does the enabling zSecure of with Guardium provide?

Guardium Vulnerability Assessment Tool

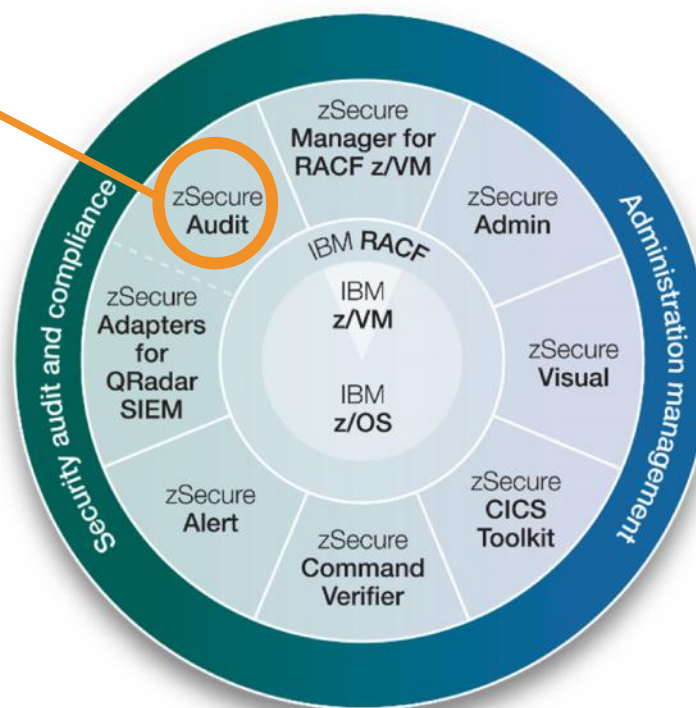
zSecure Audit:

- zSecure Audit job loads DB2 with CKADBVA tables
- Date and time of zSecure extract for each DB2 region
- User, Group and Connect information
- Pass RACF_DB2_ACL for all supported object types, in 2 forms:
 - ACL NORMAL
 - ACL EFFECTIVE

Guardium:

- Guardium VA 9.1 inside Guardium appliance
- picks up tables if new information
- applies policy
- creates exception reports

IBM Security zSecure suite



IBM Security zSecure Audit for RACF, CA ACF2 or CA Top Secret

New zSecure VA tests on system and database privileges

TEST_ID	TEST_DESC
2387	zSecure Restrict system privilege - ACCESSCTRL Authority
2388	zSecure Restrict system privilege - ARCHIVE Authority
2389	zSecure Restrict system privilege - BINDADD Authority
2390	zSecure Restrict system privilege - BINDAGENT Authority
2391	zSecure Restrict system privilege - BSDS Authority
2392	zSecure Restrict system privilege - CREATE_SECURE_OBJECT Authority
2393	zSecure Restrict system privilege - CREATEALIAS Authority
2394	zSecure Restrict system privilege - CREATEDBA Authority
2395	zSecure
2396	zSecure
2397	zSecure
2398	zSecure
2399	zSecure
2400	zSecure
2401	zSecure
2402	zSecure
2403	zSecure
2404	zSecure
2405	zSecure
2406	zSecure
2407	zSecure
2408	zSecure
2409	zSecure
2410	zSecure
2411	zSecure
2412	zSecure
2413	zSecure

TEST_ID	TEST_DESC
2438	zSecure Restrict database privilege - CREATETAB Authority
2439	zSecure Restrict database privilege - CREATETS Authority
2440	zSecure Restrict database privilege - DBADM Authority
2441	zSecure Restrict database privilege - DBCTRL Authority
2442	zSecure Restrict database privilege - DBMAINT Authority
2443	zSecure Restrict database privilege - DISPLAYDB Authority
2444	zSecure Restrict database privilege - DROP Authority
2445	zSecure Restrict database privilege - IMAGCOPY Authority
2446	zSecure Restrict database privilege - LOAD Authority
2447	zSecure Restrict database privilege - RECOVERDB Authority
2448	zSecure Restrict database privilege - REORG Authority
2449	zSecure Restrict database privilege - REPAIR Authority
2450	zSecure Restrict database privilege - STARTDB Authority
2451	zSecure Restrict database privilege - STATS Authority
2452	zSecure Restrict database privilege - STOP Authority

15 rows fetched in 0.0090s (0.0106s)

27 New system privilege tests. These tests are looking at the effective system privileges granted to the grantee, including privileges inherited from the group. These tests check for privilege grants to: Users, universal groups, orphans, and all variations of PUBLIC grants. There is one test created for each system privilege type.

15 New database privilege tests. These tests are looking at the effective system privileges granted to the grantee...including privileges inherited from the group. These tests check for privilege grants to: Users, universal groups, orphans, and all variations of PUBLIC grants.

New zSecure VA tests on database privileges

15 New database privilege tests. These tests are looking at the effective system privileges granted to the grantee...including privileges inherited from the group. These tests check for privilege grants to: Users, universal groups, orphans, and all variations of PUBLIC grants.

TEST_ID	TEST_DESC
2438	zSecure Restrict database privilege - CREATETAB Authority
2439	zSecure Restrict database privilege - CREATETS Authority
2440	zSecure Restrict database privilege - DBADM Authority
2441	zSecure Restrict database privilege - DBCTRL Authority
2442	zSecure Restrict database privilege - DBMAINT Authority
2443	zSecure Restrict database privilege - DISPLAYDB Authority
2444	zSecure Restrict database privilege - DROP Authority
2445	zSecure Restrict database privilege - IMAGCOPY Authority
2446	zSecure Restrict database privilege - LOAD Authority
2447	zSecure Restrict database privilege - RECOVERDB Authority
2448	zSecure Restrict database privilege - REORG Authority
2449	zSecure Restrict database privilege - REPAIR Authority
2450	zSecure Restrict database privilege - STARTDB Authority
2451	zSecure Restrict database privilege - STATS Authority
2452	zSecure Restrict database privilege - STOP Authority

15 rows fetched in 0.0090s (0.0106s)

Guardium Vulnerability Assessment – Report

Current Test Results

IBM InfoSphere™ Guardium™

Results for Security Assessment: **SQL Server Assessment**

Assessment executed 2010-08-27 13:30:06.0
 From: 2010-08-07 13:30:06.0
 To: 2010-08-27 13:30:06.0
 Client IP or IP subnet: Any
 Server IP or IP subnet: Any

-- Select a result --
Download PDF

Tests passing: **57%**
*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practices. Refer to the recommendations of the individual tests to learn how you can achieve best-practice status. You should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)
[Jump to Datasource list](#)

Result Summary Showing 95 of 95 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	1p 3f	15p 8f	--	1f	--
Authentication	--	2f	3p 1f	--	--
Configuration	1p	--	13p 14f 14e	--	--
Version	--	--	1p 1f	--	--
Other	1p	--	4p 2f 1e 1p 2f	1p	-- 4p 1e

Assessment Result History

Current filtering applied:

Test Severities: - Show All -
 Datasource Severities: - Show All -
 Scores: - Show All -
 Types: - Show All -

Reset Filtering Filter / Sort Controls

Assessment Test Results Compare with other results Showing 95 of 95 results (0 filtered)

Test / Datasource	Result
No Individual User Access To syscomments And sp_helptext Test category: Priv. Severity: Critical This test checks for grants on SYS COMMENTS.TEXT. Such grants allow any user to read the text comments associated with a database object, making the text publicly viewable. Ext. Reference: A Guide to Security Auditing 10.10.9.251-sa Datasource type: MS SQL SERVER Severity: None	Fail Code visibility vulnerability found Recommendation: Privilege on syscomments and sp_helptext has been granted. These objects contains sensitive database information which should not be publicly available. We recommend that you revoke these privileges.
No Select Privileges On System Tables/Views In Application Databases Test category: Priv. Severity: Critical This test checks for grants of the SELECT privilege on system tables in application databases. Users with these privileges have access to sensitive	Fail Some application databases have SELECT privileges granted to system tables: Sensitedb: public(119), ReportServer: public(119), financial: public(119), ReportServerTempDB: public(119). Recommendation: SELECT privileges have been granted on system tables in application databases other than master, msdb, and tempdb. We recommend that you revoke these

Result History

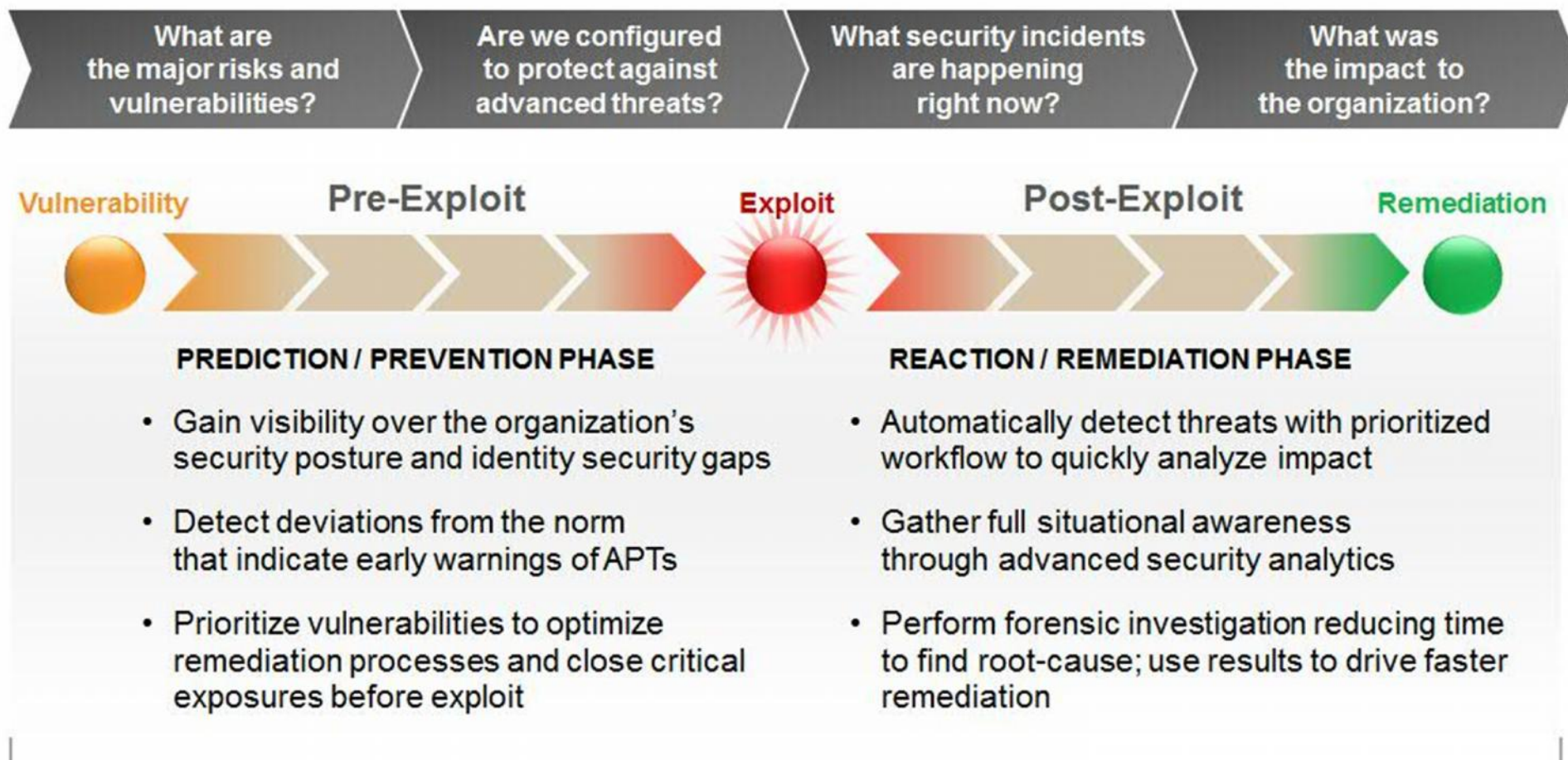
Prioritized Breakdown

Filters and Sort Controls

Detailed Test Results

Detailed Remediation Suggestions

Security solutions must address the Security Intelligence timeline



Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

QRadar provides security visibility and Security Intelligence

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



Identity and User Context

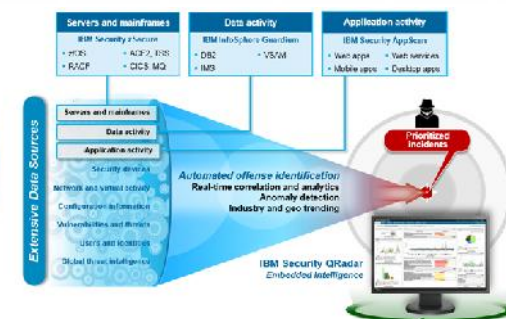
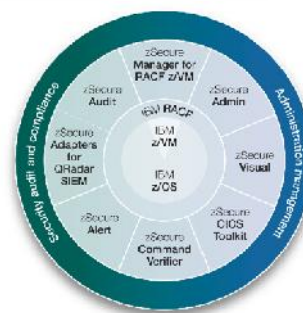
Real-time Network Visualization and Application Statistics

Inbound Security Events

Value of zSecure integration with QRadar

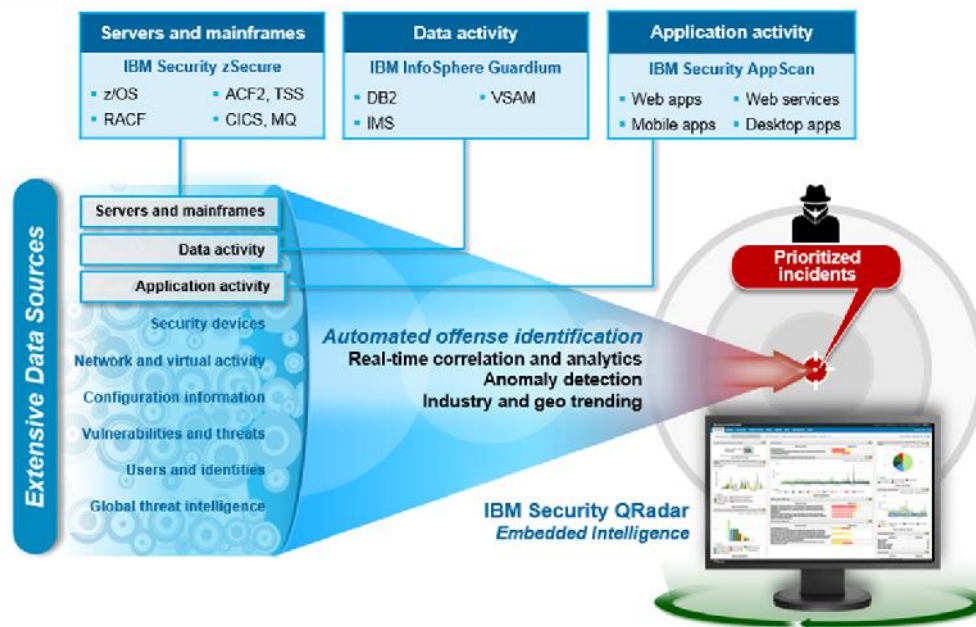
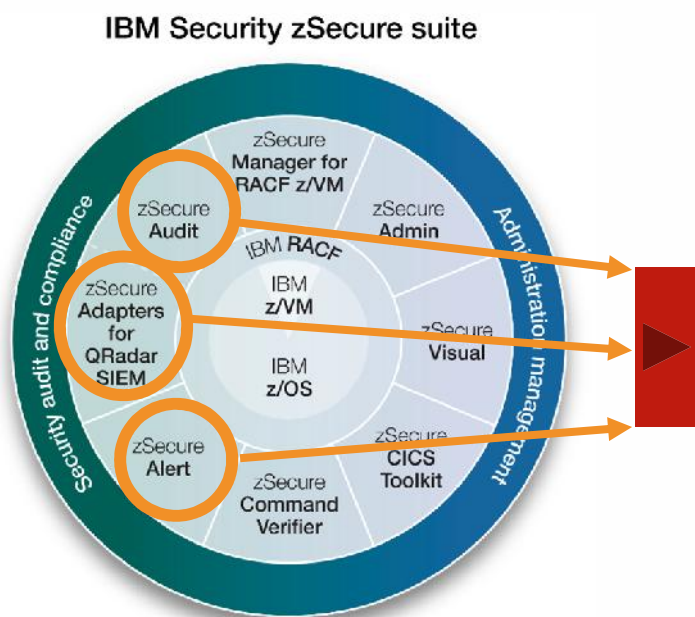
- Plugs a hole in the Enterprise Security Monitoring practice
- Provides a holistic, centralised approach for Security Monitoring
- Supports separation of duties – stop the legacy practice of self-policing!
- Maximize QRadar capabilities for:

- Log management
- Security Information and Event Management
- Anomaly detection
- Incident forensics
- Configuration Management
- Vulnerability Management
- Risk management



- Enhances the monitoring experience with graphical displays and user friendly reporting
- Extend best practices and comply with regulatory/legal/compliance requirements

The zSecure products that enable integration with QRadar



Note:

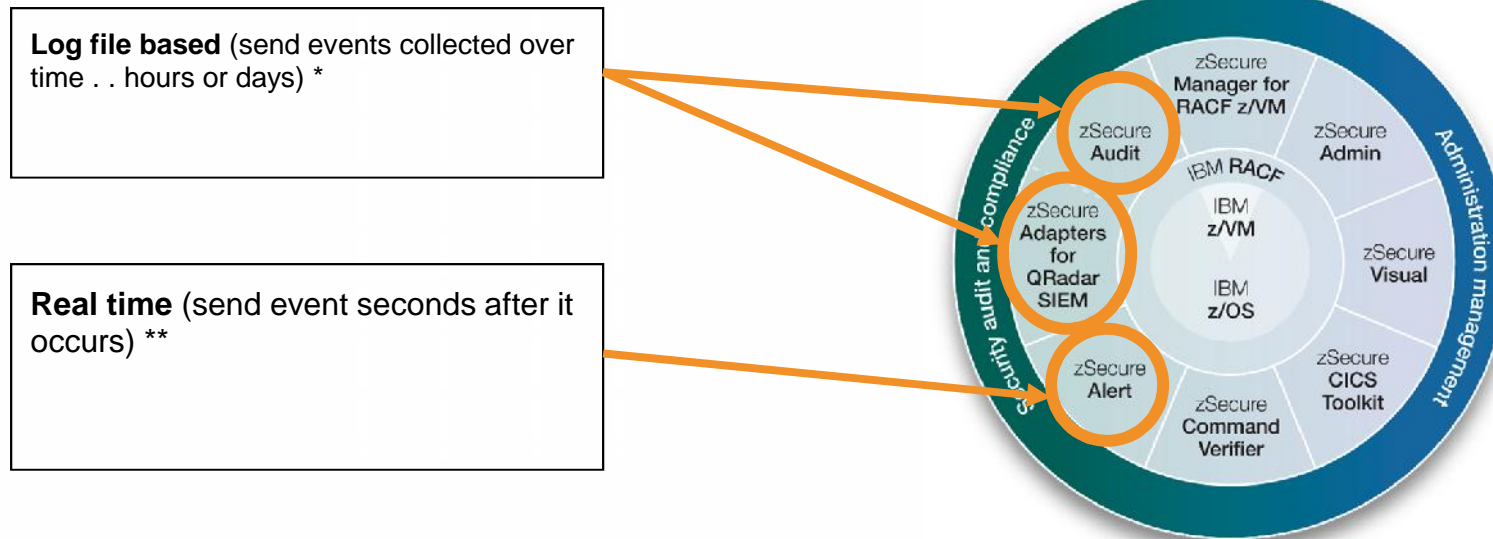
- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

Event sources from z Systems . . .



What does the enabling zSecure products deliver?

IBM Security zSecure suite

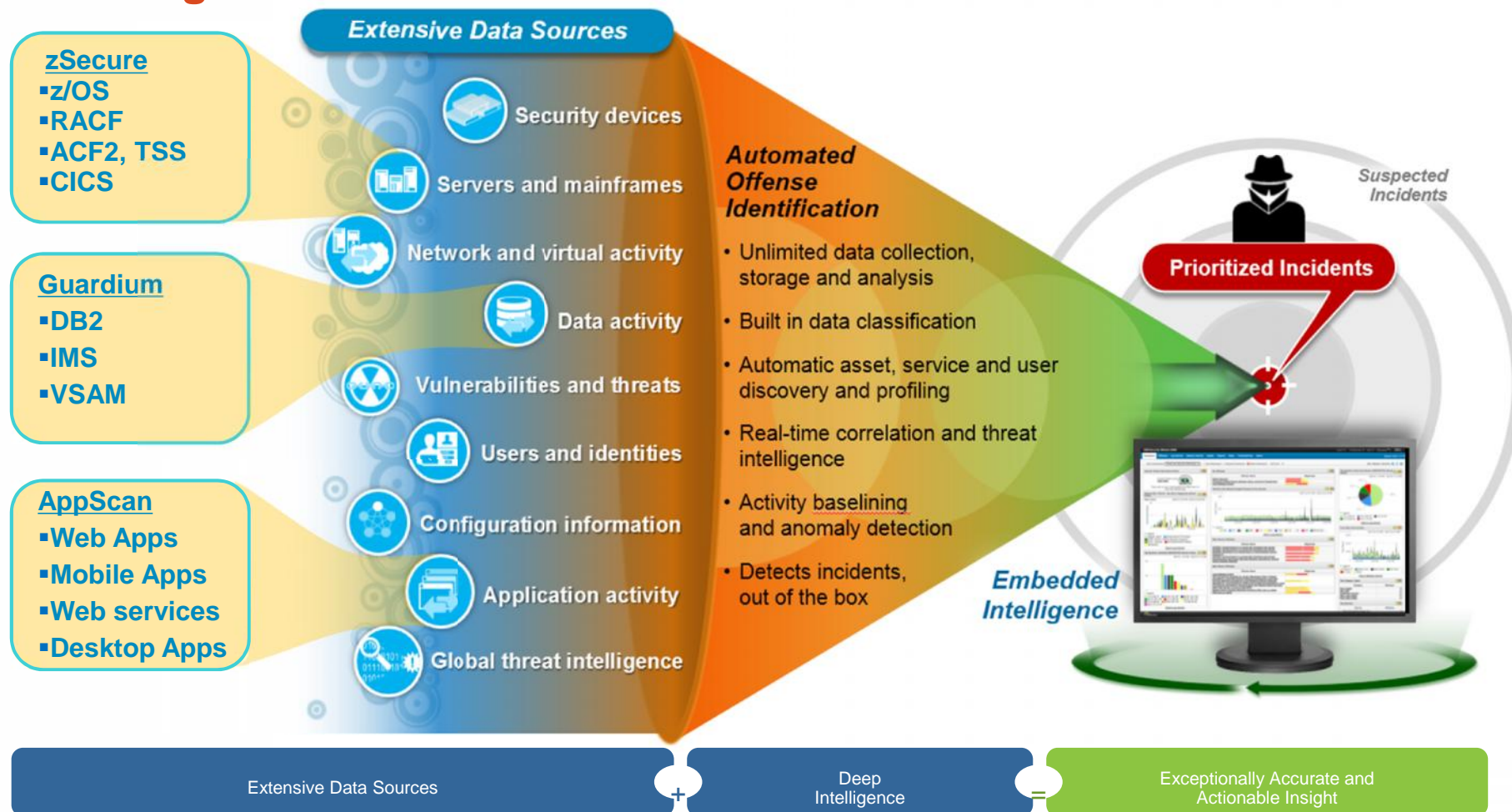


Log file based (send events collected over time . . . hours or days) *

Real time (send event seconds after it occurs) **

- * IBM Security zSecure Audit for RACF or CA ACF2 or CA Top Secret
- * IBM Security zSecure Adapters for QRadar SIEM
- ** IBM Security zSecure Alert for RACF or CA ACF2

zSecure, Guardium, AppScan & QRadar improve your Security Intelligence



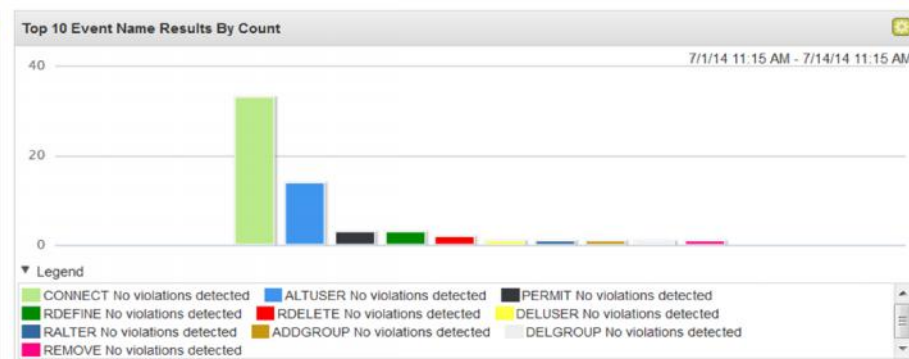
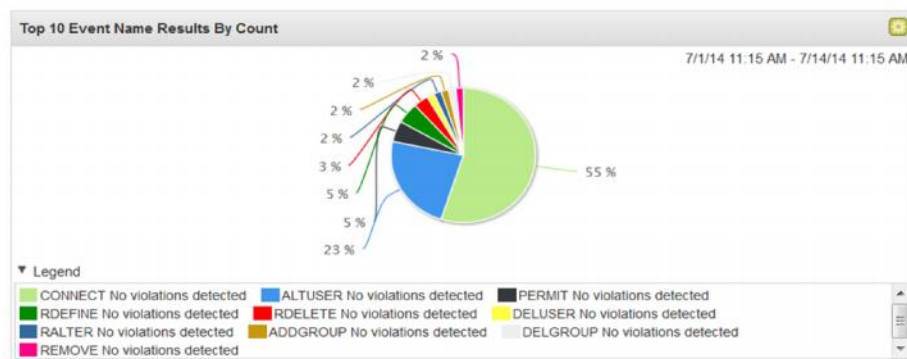
✓ Centralized views; automatic alerts; increased accuracy; simplified compliance

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(SYSPROC) 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 detected	Multiple (33)	7/1/14, 11:35:28 AM	PEASEJ	JAZZ03 RACF	Multiple (32)	Success	User Account Changed	33
ALTUSER No violations detected	Multiple (6)	7/1/14, 11:35:28 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	User Account Changed	14
PERMIT No violations detected	Multiple (3)	7/1/14, 11:35:29 AM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDEFINE No violations detected	Multiple (3)	7/1/14, 11:35:30 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDELETE No violations detected	Multiple (2)	7/1/14, 11:35:31 AM	Multiple (2)	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
DELUSER No violations detected	DELUSER DEMOUSER	7/1/14, 11:35:32 AM	PEASEJ	JAZZ03 RACF	DEMOUSER	Success	User Account Removed	1

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

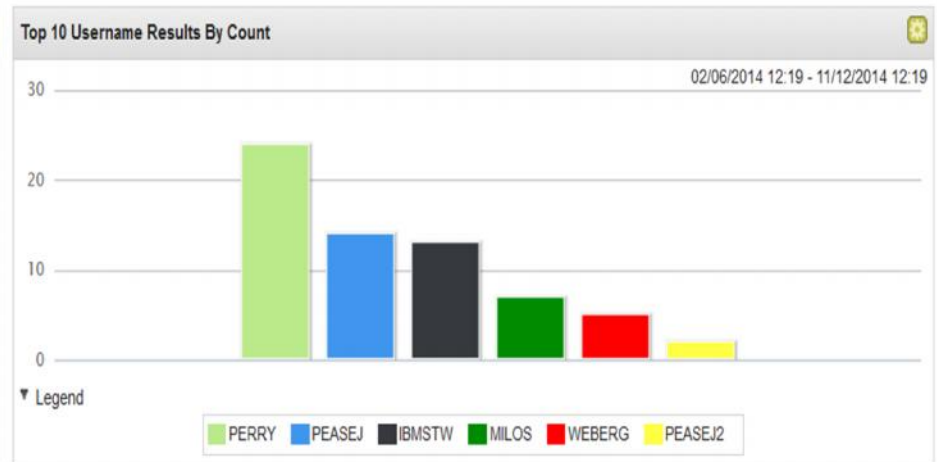
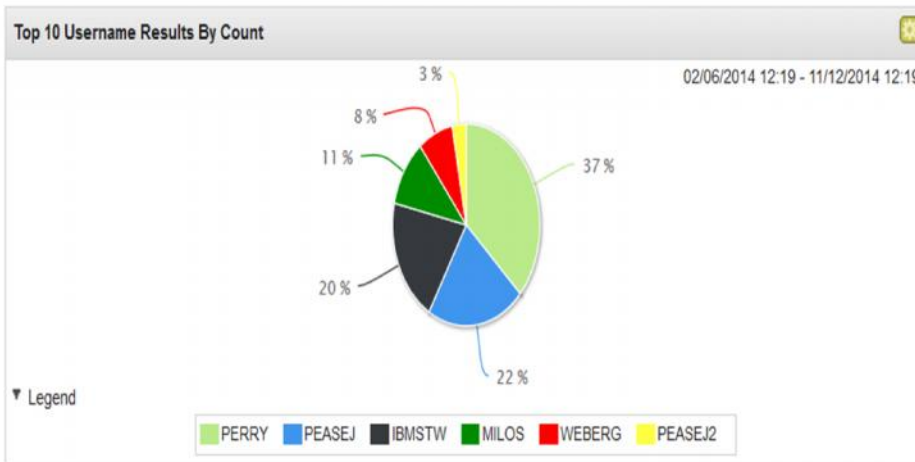
Systems Programmer
accesses a Payroll file on the
mainframe

```

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  GB00N883  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)	Count
PERRY	LUIGI PERRONE	RACHECK Successf...	25 Sep 2014 16:47:16	JAZZ03 RACF	DATASET	Multiple (3)	Multiple (2)	Multiple (2)	InstSpecRd	
PEASEJ	JAMIE PEASE	RACHECK Successf...	2 Jul 2014 10:20:25	JAZZ03 RACF	Multiple (2)	Multiple (3)	Multiple (2)	Multiple (2)	Multiple (2)	
IBMSTW	STEVE TALBOT-WAL...	RACHECK Successf...	22 Sep 2014 07:56:53	JAZZ03 RACF	Multiple (2)	Multiple (4)	Multiple (2)	Multiple (2)	Multiple (2)	
MILOS	Multiple (2)	RACHECK Successf...	14 Oct 2014 12:54:43	JAZZ03 RACF	DATASET	PAYROLL EMPLOYEE SALARY	Multiple (2)	ALTER	InstSpecRd	
WEBERG	GUENTER WEBER	RACHECK Successf...	4 Nov 2014 13:17:14	JAZZ03 RACF	DATASET	Multiple (2)	READ	ALTER	InstSpecRd	
PEASEJ2	JAMIE PEASE 2	RACHECK Successf...	17 Sep 2014 15:55:16	JAZZ03 RACF	DATASET	PAYROLL EMPLOYEE ADDRESS	Multiple (2)	ALTER	InstSpecRd	

Who accessed the sensitive resource

What they accessed

Resource is sensitive for read access

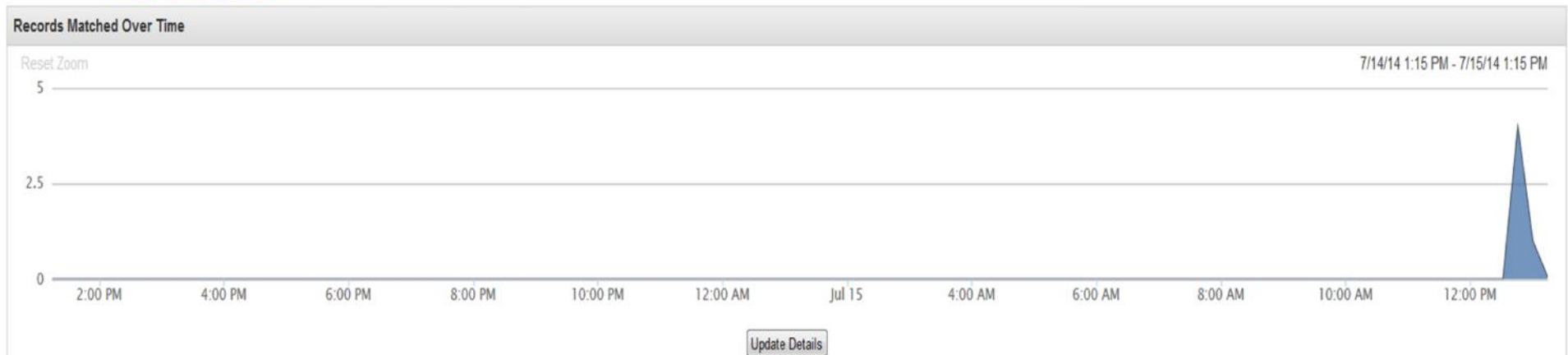
Scenario # 1 – Monitoring inappropriate access to sensitive data

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 – Monitoring Privileged User activities in QRadar



(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!

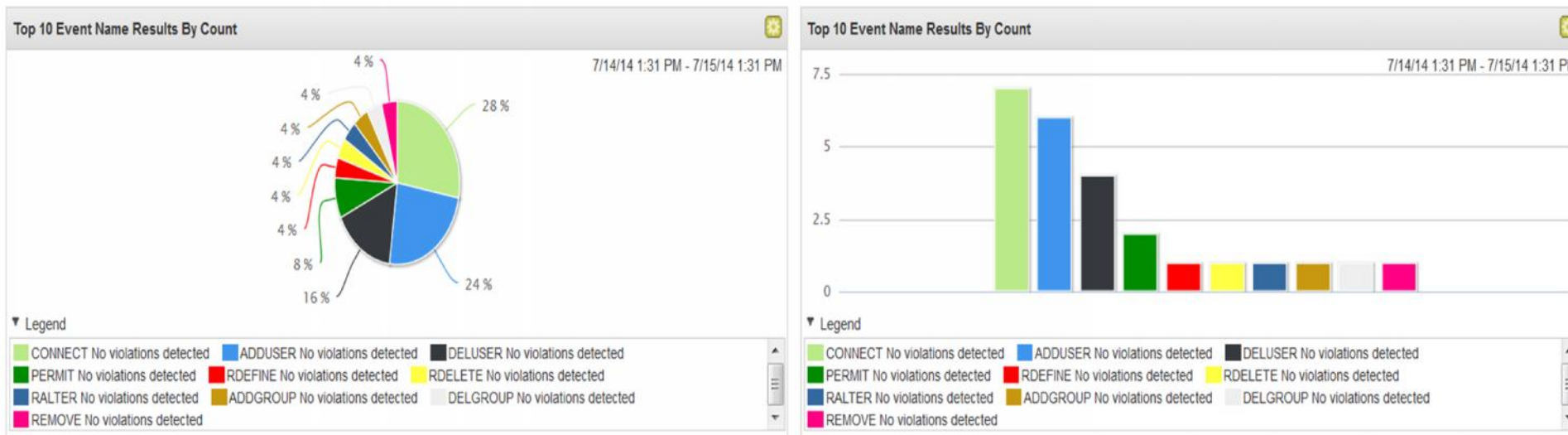
Scenario # 3 – Security Administrator activities occurring on System z

```
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 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

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!

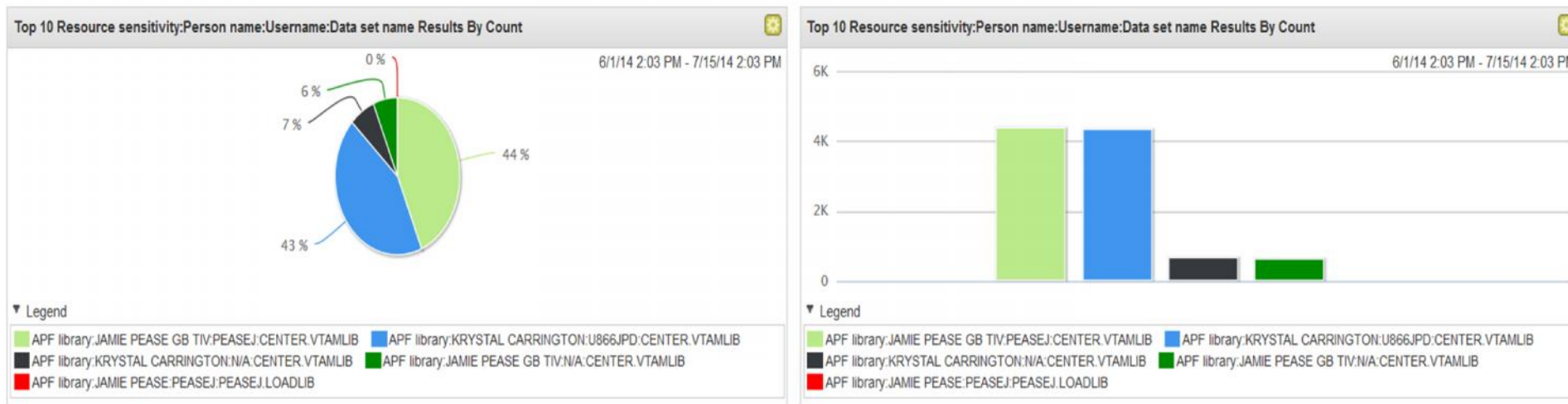
Event data collected by **zSecure Audit**

Scenario # 3 – Monitoring Security Administrator activities

Low Level Category	User Account Added					<div style="border: 1px solid black; background-color: #ADD8E6; padding: 5px; display: inline-block;">Drill down</div>					
Event Description	ADDUSER No violations detected										
Magnitude		(2)	Relevance	1	Severity	1	Credibility	5			
Username	PEASEJ										
Start Time	Jul 15, 2014, 1:03:38 PM		Storage Time	Jul 15, 2014, 1:03:38 PM		Log Source Time	Jul 15, 2014, 12:50:24 PM				
Access allowed (custom)	N/A										
Access intent (custom)	N/A										
Access of unix ACL group (custom)	N/A										
Access of unix ACL user (custom)	N/A										
Application name (custom)	N/A										
Command (custom)	ADDUSER DEMOUSER AUTHORITY(USE) DFLTGRP(SYSPROG) NOADSP NOAUDITOR NOCLAUTH NOGRPACC NOOIDCARD NOOPERATIONS NORESTRICTED NOSPECIAL OWNER(SYSPROG) PASSWORD(<password>) UACC(NONE)										

The actual RACF command that was executed by the Security Administrator

Scenario # 4 – Monitoring your Systems 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

Scenario # 4 – Monitoring your System Programmers

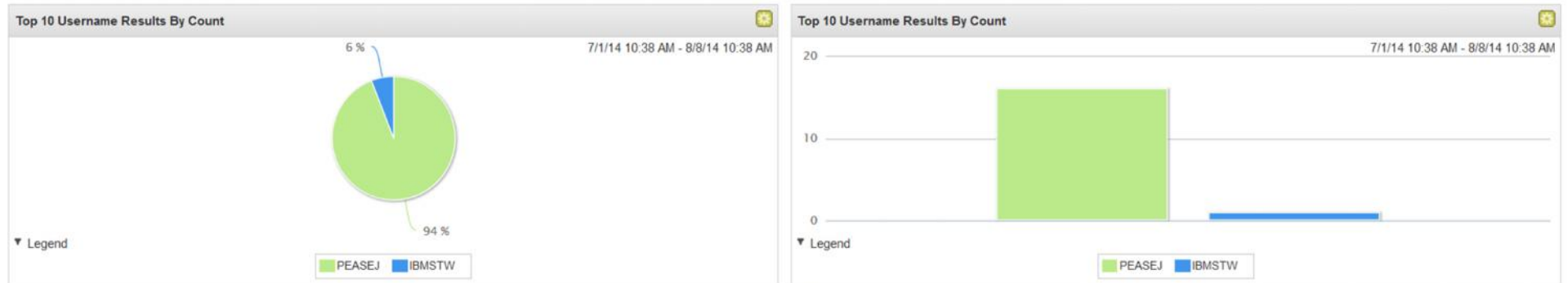
Resource sensitivity (custom)	APF library
SAF Class (custom)	DATASET
SAF resource name (custom)	PEASEJ.LOADLIB
SNA terminal name (custom)	ISZ004
Sensitive groups (custom)	N/A
Sensitive user privileges (custom)	special auditor
Submitted by (custom)	N/A
System SMF id (custom)	ZT01
System/job (custom)	ZT01 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
-----------	--------------

Scenario # 5 – Keeping track of Security Violations



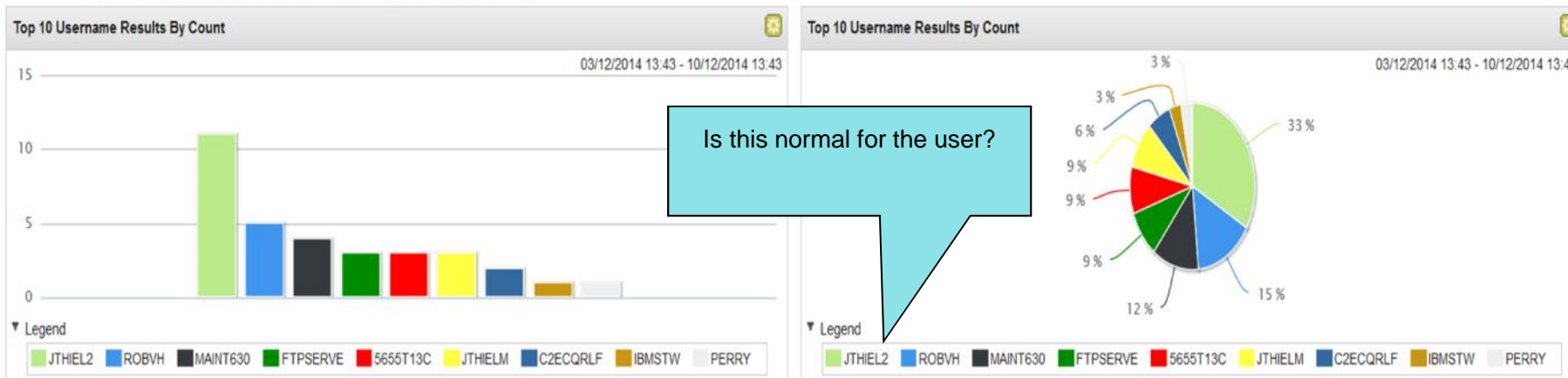
(Hide Charts)

Username	Person name (Unique Count)	Event Name (Unique Count)	Log Source Time (Minimum)	SAF Class (Unique Count)	SAF resource name (Unique Count)	Access intent (Unique Count)	Access allowed (Unique Count)	Resource sensitivity (Unique Count)	Count
PEASEJ	JAMIE PEASE	RACHECK Insufficient a...	7/2/14, 10:20:22 AM	DATASET	Multiple (2)	READ	NONE	Sens read	
IBMSTW	STEVE TALBOT-WALSH	RACHECK Insufficient a...	8/5/14, 6:43:46 AM	DATASET	IBMZSEC.DATA.PAYROLL	READ	NONE	Sens read	

A view of security violation for sensitive application datasets

Application data is sensitive for read access

Scenario # 6 – Spot trends in behaviour amongst infrastructure staff



Is this normal for the user?

(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)	Count
JTHIEL2	JAN THIELMANN 2	RACHECK Insufficient...	5 Dec 2014 16:12:12	JAZZ03 RACF	Multiple (3)	Multiple (3)	READ	NONE	Multiple (3)	
ROBVH	ROB VAN HOBOKEN	RACHECK Insufficient...	28 Nov 2014 17:54:06	Multiple (2)	Multiple (2)	Multiple (5)	Multiple (2)	NONE	None	
MAINT630	None	RACHECK Insufficient...	26 Nov 2014 18:43:42	zVM63A1	SURROGAT	LOGONBYMAINT630	READ	NONE	None	
FTPSERVE	None	RACHECK Insufficient...	8 Dec 2014 13:44:53	zVM63A1	VMBATCH	ROBVH	CONTROL	NONE	None	
5655T13C	None	RACHECK Insufficient...	28 Nov 2014 14:22:45	zVM63A1	VMMDISK	Multiple (3)	Multiple (2)	NONE	None	
JTHIELM	JAN THIELMANN	RACHECK Insufficient...	5 Dec 2014 16:25:06	JAZZ03 RACF	XFACILIT	C4R.DATASET=NOCHANGE.SY...	UPDATE	NONE	None	
C2ECQRLF	None	RACHECK Insufficient...	8 Dec 2014 15:08:50	JAZZ03 RACF	DATASET	ROBVH.CKRPARM	READ	NONE	None	

Scenario # 7 – Who used FTP to transfer sensitive data?

Username	Source IP (Unique Count)	Destination IP (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Magnitude (Maximum)	Event Count (Sum)
QRADFTP	Multiple (2)	9.212.143.76	JAZZ03 zOS	Multiple (6)	4	11,389
TWSE2E	9.212.143.76	9.212.143.76	JAZZ03 zOS	Multiple (2)	2	3
C2PSUSER	9.212.143.76	9.212.143.76	JAZZ03 zOS	System Configuration	2	2
PEASEJ	9.212.143.76	9.212.143.123	JAZZ03 zOS	Unknown	3	1

Username	PEASEJ				
Start Time	10 Dec 2014 00:32:10	Storage Time	10 Dec 2014 00:32:10	Log Source Time	9 Dec 2014 03:00:27
Access intent (custom)	N/A				
Catalog (custom)	N/A				
Command (custom)	N/A				
Completion code (custom)	N/A				
Completion status (custom)	N/A				
DD name (custom)	N/A				
Data set name (custom)	IBMZSEC.DFDSS.DUMP				
Descriptor (custom)	N/A				
Event Summary (custom)	FTP client host zt01 user PEASEJ STOR IBMZSEC.DFDSS.DUMP 245,194,349 bytes in 4.23 seconds client 9.212.143.76:220 server 9.212.143.123:222 reply 250				

Source and Destination Information

Source IP	9.212.143.76	Destination IP	9.212.143.123
------------------	--------------	-----------------------	---------------

Daily (scheduled) reporting

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

Customers typically run scheduled monitoring reports

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 viol...
- PERMIT No violati...
- ADDSD No violatio...
- DELDSD No violati...
- ADDUSER No viola...
- REMOVE No violati...
- ALTDSO No violati...
- ALTGROUP No viol...
- DELGROUP No viol...
- ADDCGROUP No vio...
- RALTER No violati...
- RDELETE No violati...
- RDEFINE No violati...

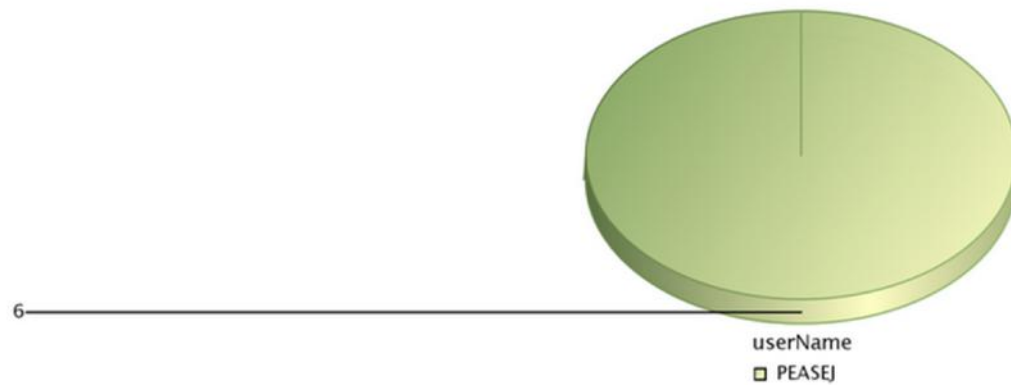
RACF Commands Z-RACF Commands

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.*' NO SET OWNER(SYS PROG)	Jul 1, 2014, 11:35:29 AM	FEASEJ	JAZZ03 RACF	DEMOUSER.WORK.*	Success	Access Permitted	1
DELDSD No violations detected	DELDSD 'DEMOUSER.WORK.*'	Jul 1, 2014, 11:35:31 AM	FEASEJ	JAZZ03 RACF	DEMOUSER.WORK.*	Success	Policy Change	1

Daily (scheduled) reporting

Access to Payroll files
Jul 15, 2014, 1:00 AM GMT+2 - Jul 15, 2014, 7:30 PM GMT+2
Count



Schedule a report to monitor who has been reading your sensitive files

Events

Access to Payroll files

Jul 15, 2014, 1:00:00 AM - Jul 15, 2014, 7:30:00 PM

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)	Count
PEASEJ	JAMIE PEASE	RACHECK Successful access	Jul 15, 2014, 12:10:08 PM	JAZZ03 RACF	DATASET	PAYROLL.EMPLOYEE.SALARY	Multiple (2)	ALTER	Sens read	6

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.

Learn more about IBM Security zSecure Solutions

[zSecure website](#)

[zSecure latest release](#)

[zSecure product library](#)

[zSecure forum](#)

[zSecure information center](#)

[zSecure Redbook](#)



Learn more about IBM Security QRadar SIEM



Visit our [Website](#)

Visit the IBM QRadar Website: <http://ibm.co/QRadar>

Learn about IBM Security zSecure Adapters for QRadar SIEM
[LINK](#)

Visit our blog: www.securityintelligence.com

Follow us on Twitter: [@ibmsecurity](https://twitter.com/ibmsecurity)

Download the 2014 Gartner Magic Quadrant for SIEM :
<http://ibm.co/U7Syom>

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2014. 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.