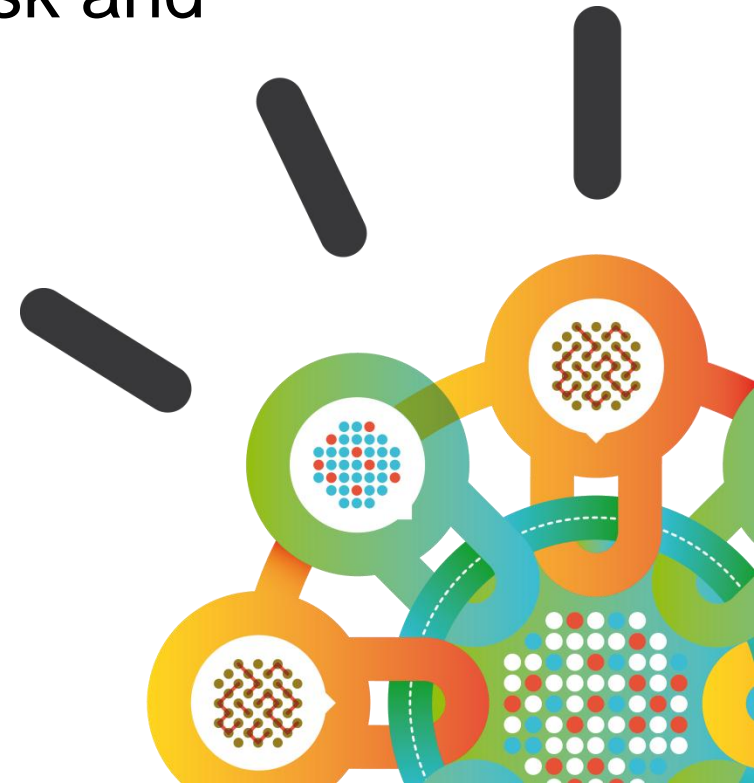


Security Intelligence.
Think Integrated.

IBM Security zSecure suite 2.1: Demonstrating Governance, Risk and Compliance on your Mainframe

October 2013

Anne Lescher – lescher@us.ibm.com



Trademark

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

BladeCenter*	IBM*	InfoSphere	System z*	zEnterprise*
CICS*	IBM (logo)*	MQSeries*	WebSphere*	z/OS*
DB2*	IMS	HiperSockets	X-Force*	zSecure*
Guardium*	Informix*	RACF*		

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Increasingly interconnected world opens the door to emerging threats and leaks...



Data Explosion

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere



Consumerization of IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared



EVERYTHING IS EVERYWHERE

Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more



Attack Sophistication

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

**You know? you can do
this online now.**





Security Challenges Specific to System z security administration

Ensuring Compliance



Increasing Complexity



Rising Costs



Visibility



■ Compliance:

- Compliance verification is a manual task with alerts coming after a problem has occurred, if at all

■ Complexity:

- The mainframe is an integral component of many large business services, making the identification and analysis of threats very complex and creating a higher risk to business services
- Systems are vulnerable to the unmanaged activities of privileged users.

■ Cost:

- Mainframe security administration is usually a manual operation, or relies upon old, poorly documented scripts.
- Administration is done by highly skilled mainframe resources that are usually in short supply.

■ Visibility:

- Mainframe processes, procedures, & reports are often siloed from the rest of the organization

IBM's security framework... Intelligence Integration Expertise



- 

Security Intelligence and Analytics
Optimize security management with additional context, automation and integration across domains
- 

People
Mitigate the risks associated with user provisioning and access to corporate resources
- 

Data
Understand, deploy, and properly test controls for access to and usage of sensitive data
- 

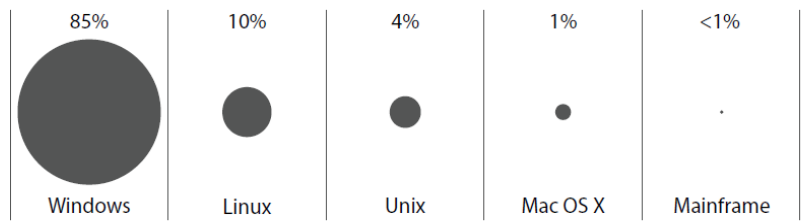
Applications
Keep applications secure, protected from malicious or fraudulent use, and hardened against failure
- 

Infrastructure
Help protect and maintain compliance of networks, servers, storage, endpoints and mobile devices

IBM System z & Security

- A strong heritage of being an extremely securable platform for virtual environments and workloads
 - Security is built into every level of the System z structure
 - Processor
 - Hypervisor
 - Operating system
 - Communications
 - Storage
 - Applications
 - Security features designed specifically to help users comply with security related regulatory requirements, including identity and access management; hardware and software encryption, communication security capabilities; and extensive logging and reporting of security events
 - Extensive security certifications (e.g., Common Criteria and FIPS 140) including EAL5+

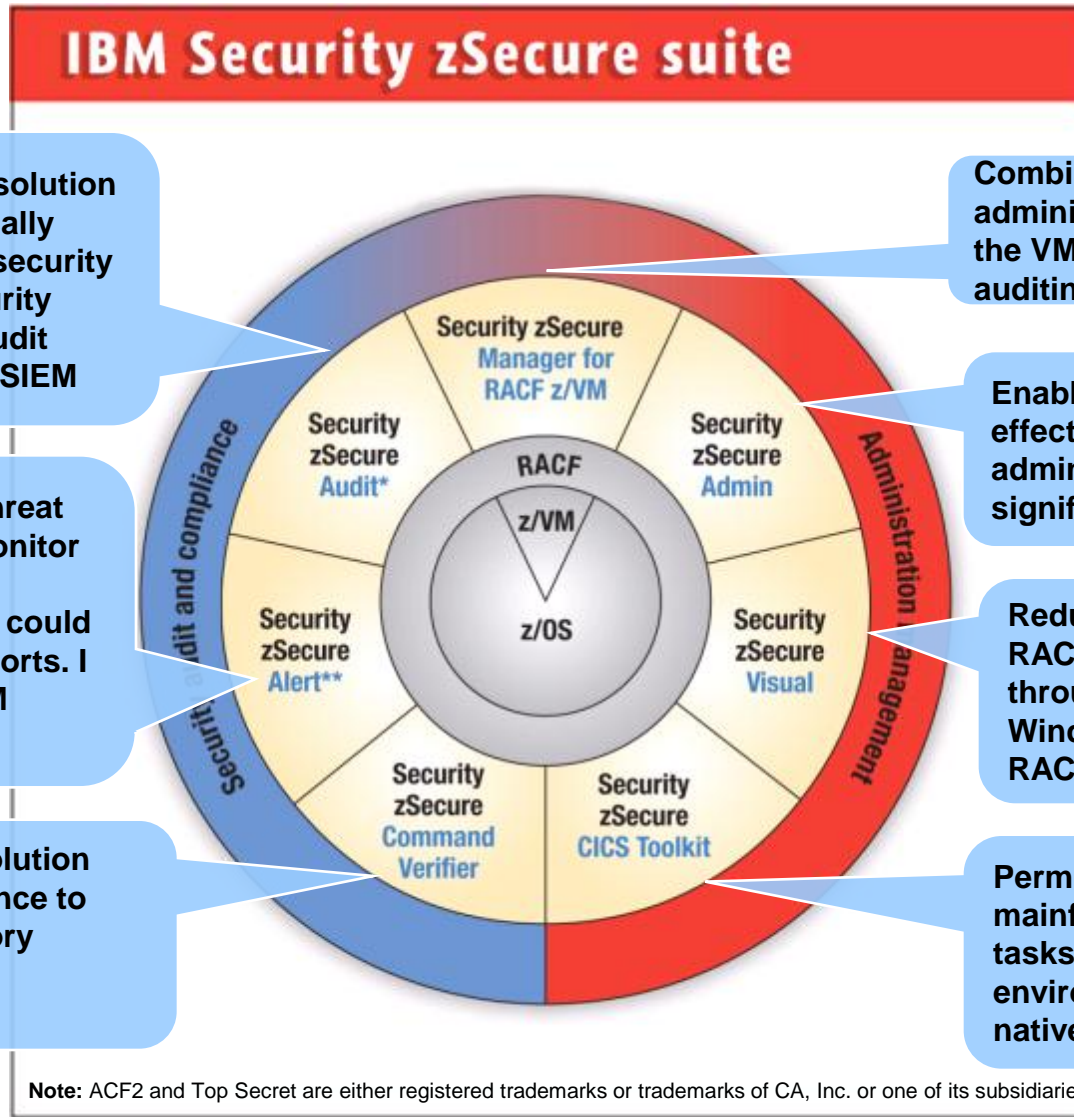
Distribution of Data Breaches by Operating Systems



Source: Verizon 2011 Data Breach Investigations Report



IBM Security zSecure Suite Overview



Compliance and audit solution that helps to automatically analyze and report on security events and detect security exposures. Provides audit information to QRadar SIEM

Real-time mainframe threat monitoring helps to monitor intruders and identify misconfigurations that could hamper compliance efforts. Provides alerts to SIEM products.

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

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

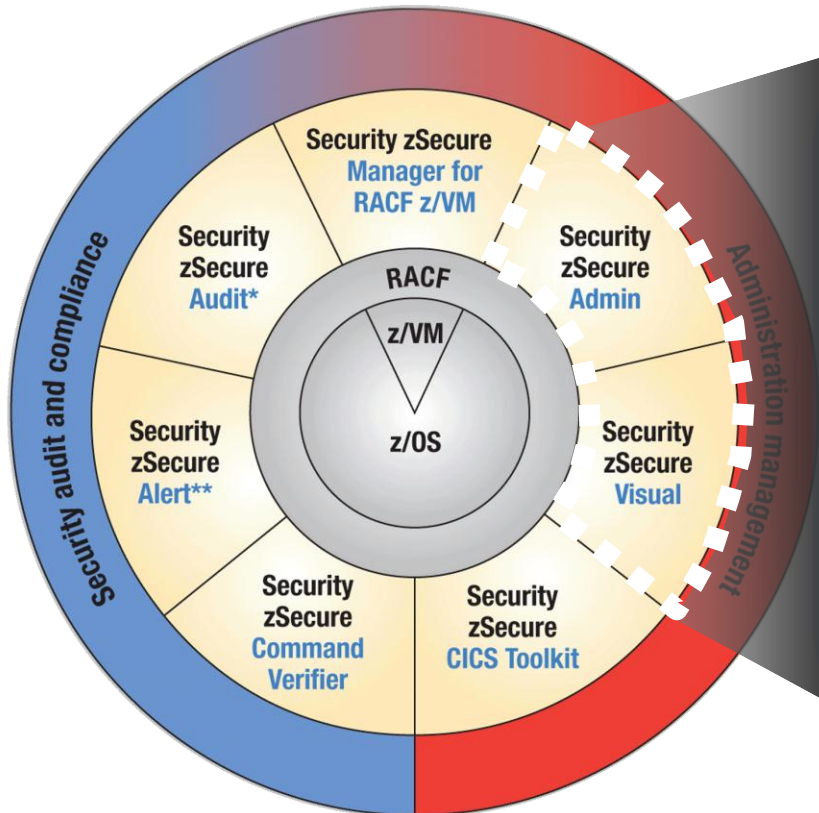
Enables more efficient and effective RACF administration, using significantly fewer resources

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

Permits you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

IBM Security zSecure suite – Administration

IBM Security zSecure Suite



IBM Security zSecure Administration

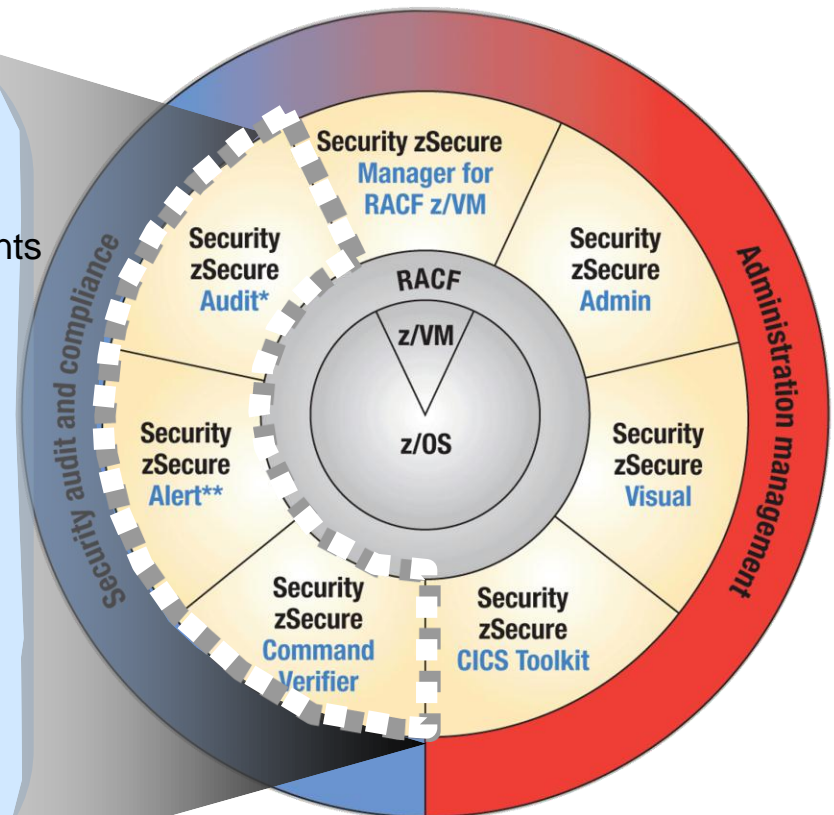
- ✓ zSecure Admin:
 - Improves security at lower labor cost
 - Also saves cost by:
 - Avoiding configuration errors
 - Improving directory merges
 - Efficient group management
- ✓ zSecure Visual:
 - Permits changes in minutes vs. overnight
 - Provides access for only current employees & contractors (better business control)
 - Enables segregation of duties (minimizing business risk)
 - Aids in reducing labor cost and errors

IBM Security zSecure suite – Compliance and Auditing

IBM Security zSecure Suite

IBM Security zSecure Compliance and Auditing

- ✓ zSecure Audit* :
 - Reports can match business model/requirements
 - Prioritizes tasks (optimize labor utilization)
 - Helps find “segregation of duties” exposures (reduces risk)
- ✓ zSecure Alert** :
 - Allows capture of unauthorized “back door” changes to RACF / security policies
 - Addresses real time audit control points, especially network audit control points
- ✓ zSecure Command Verifier
 - Audits RACF admins’ changes
 - Offers security monitoring without additional CPU/cost
 - Audit in seconds vs. days

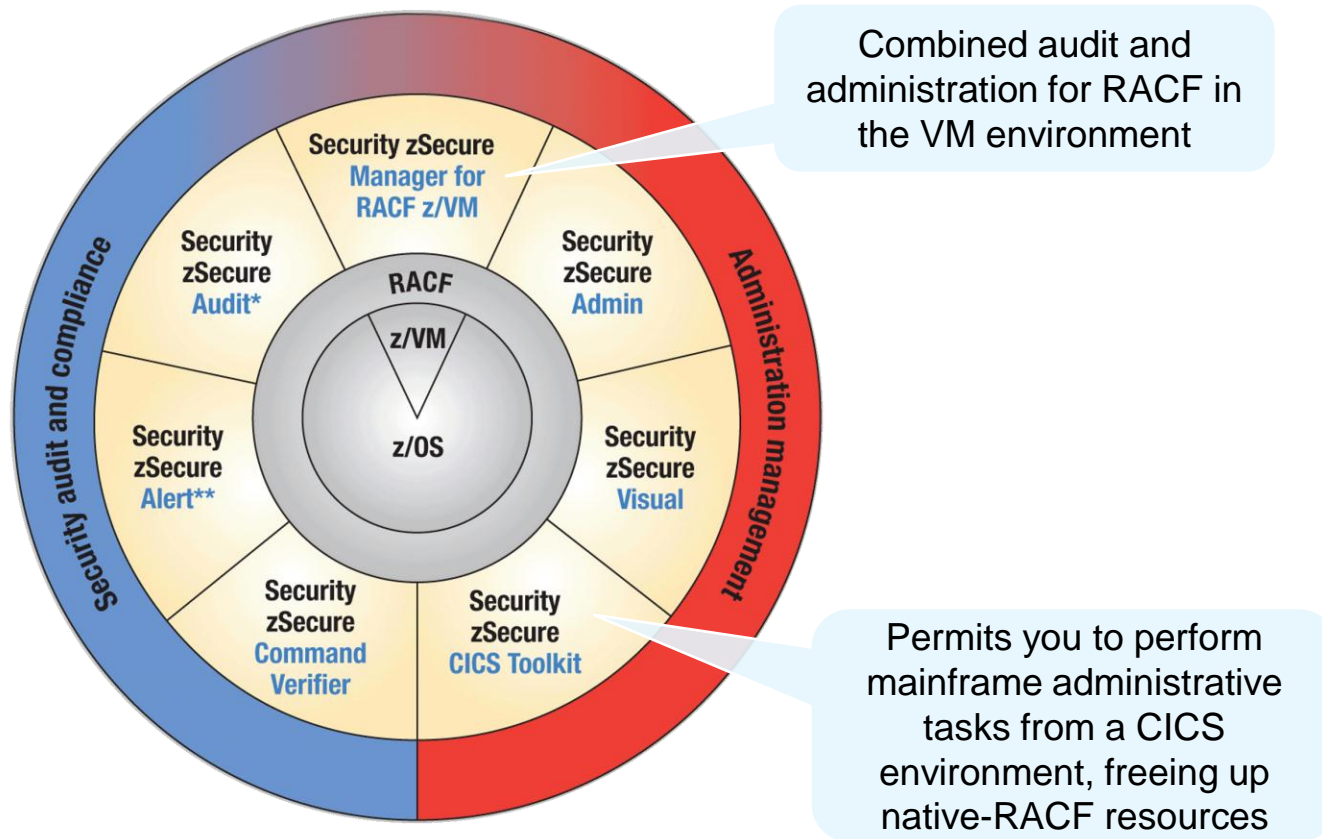


*Also available for ACF2™ and Top Secret®

**Also available for ACF2

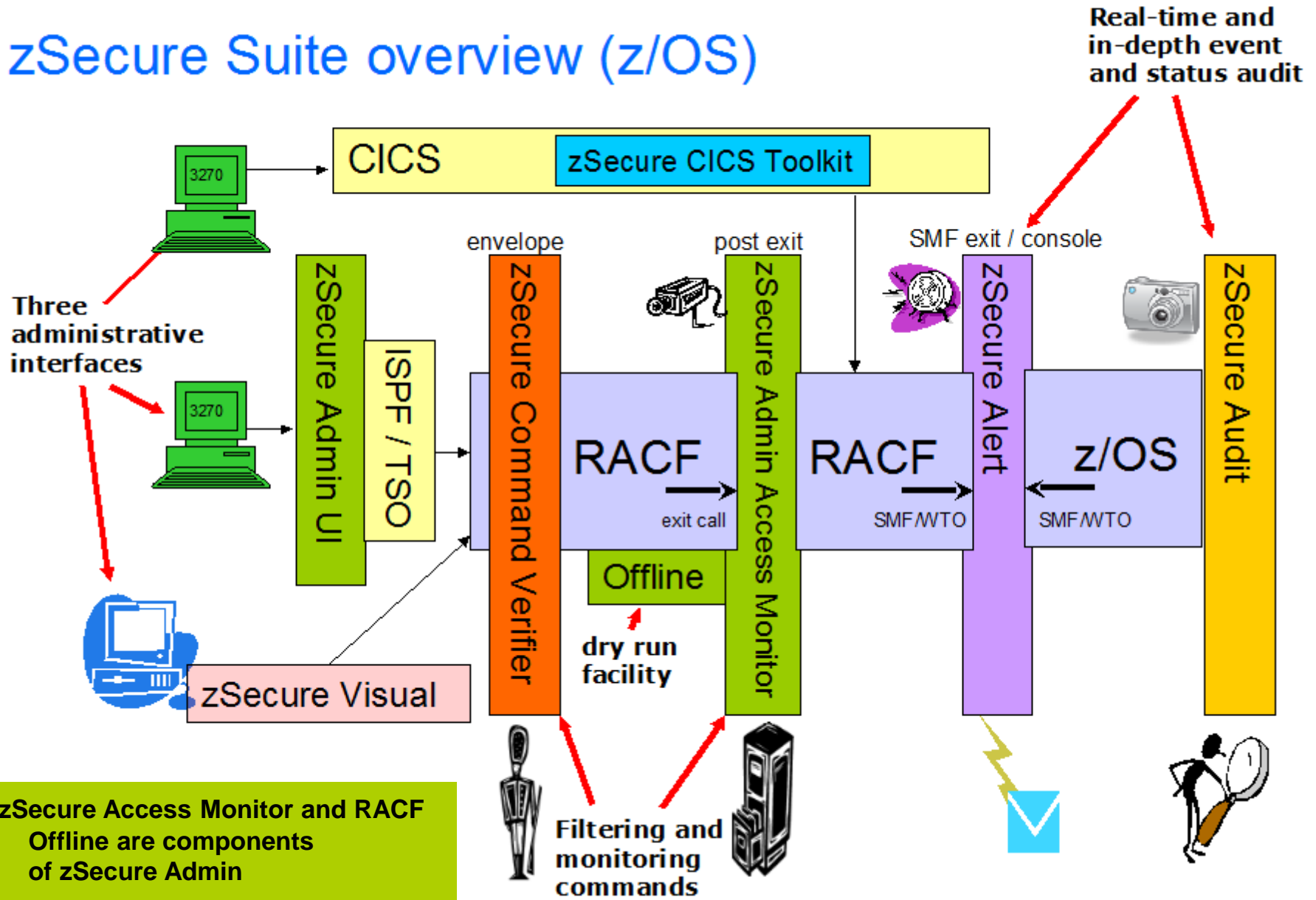
IBM Security zSecure suite Overview

IBM Security zSecure Suite



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

zSecure Suite overview (z/OS)



What's new in zSecure 2.1- Themes

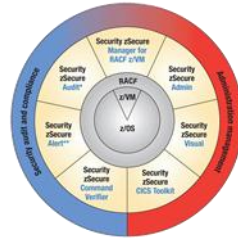
Key solution highlights

- **Enhanced automated auditing & monitoring support for regulatory compliance**
 - provide the capability to improve results through a comprehensive, automated audit referencing a built-in knowledge base
 - reduce the manual processes for gathering data to support activities for compliance
- **New Digital Certificates management for improved security and reduced complexity**
 - ease of creating, administering, customizing and auditing digital certificates
 - enable user ID tracking in Access Monitor for improved visibility and certificate usage
- **Integrated mainframe security intelligence with QRadar SIEM**
 - enrich real-time collection, normalization & analysis of RACF events to reduce manual security operations
- **Ease of multiple RACF system security administration**
- **z/OS V2R1 currency**

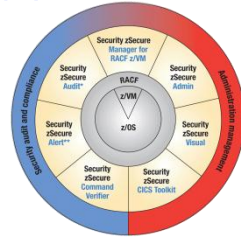


zSecure What's new in 2.1

- DB2 resource collection/reporting
- Certificate management support
- Access Monitor improvements
- Compliance Testing Framework
- FTP daemon security settings
- TN3270 security settings
- ISPF UI enhancements
- CARLa enhancements
- Other Enhancements
 - zSecure Visual enhancements
 - zSecure Server enhancements



Expanded integration points with DB2 for enhanced compliance



■ Features

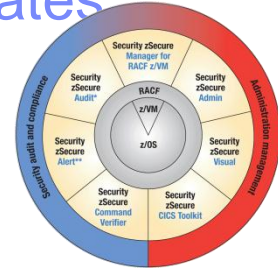
- Collect data from additional DB2 object types, primarily related to access levels
- Collect data from DB2 Internal Access Control Lists to track effective access
- Collect data on potential conflicts between DB2 Internal Access Control Lists and RACF

■ Benefits

- More effective audit of database access improves integrity of DB2 databases
- Reduces requirements for manual audits of DB2 access therefore reduction in personnel resource requirements



Enhanced support for administration of RACF digital certificates



- RACF Digital Certificates
 - Digital Certificates are used for enhance authentication, verification, and encryption
 - RACF supports digital certificates for use with z/OS
- Features
 - New facility to create, administer, customize and audit RACF digital certificates
 - New Facility to create certificate templates to pre-fill parameters according to business purposes
 - User-id tracking and monitoring of digital certificate usage
- Benefits
 - Greatly eases administration for customers already using digital certificates
 - Encourages adoption of digital certificates for customers who are not yet exploiting them

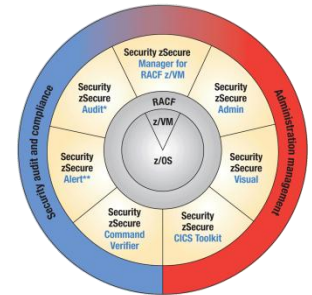
Extended Access Monitor access usage

■ Features

- Various performance improvements
- Richer data collection
- Enhanced RACINIT support
- Support for digital certificates
- Ability to identify and remove unused logon ids

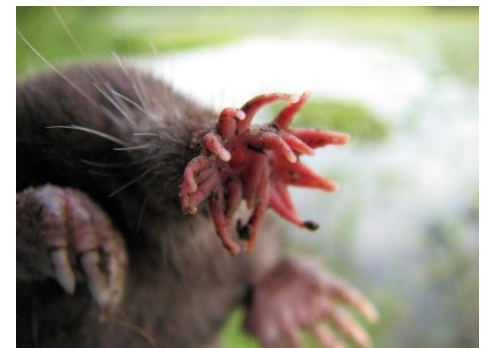
■ Benefits

- Improves integrity of RACF databases thus improving integrity of z/OS
- Improved performance means greater adoption of Access Monitor which improves z/OS integrity



Condylura
Cristata
(Star Nosed
Mole)

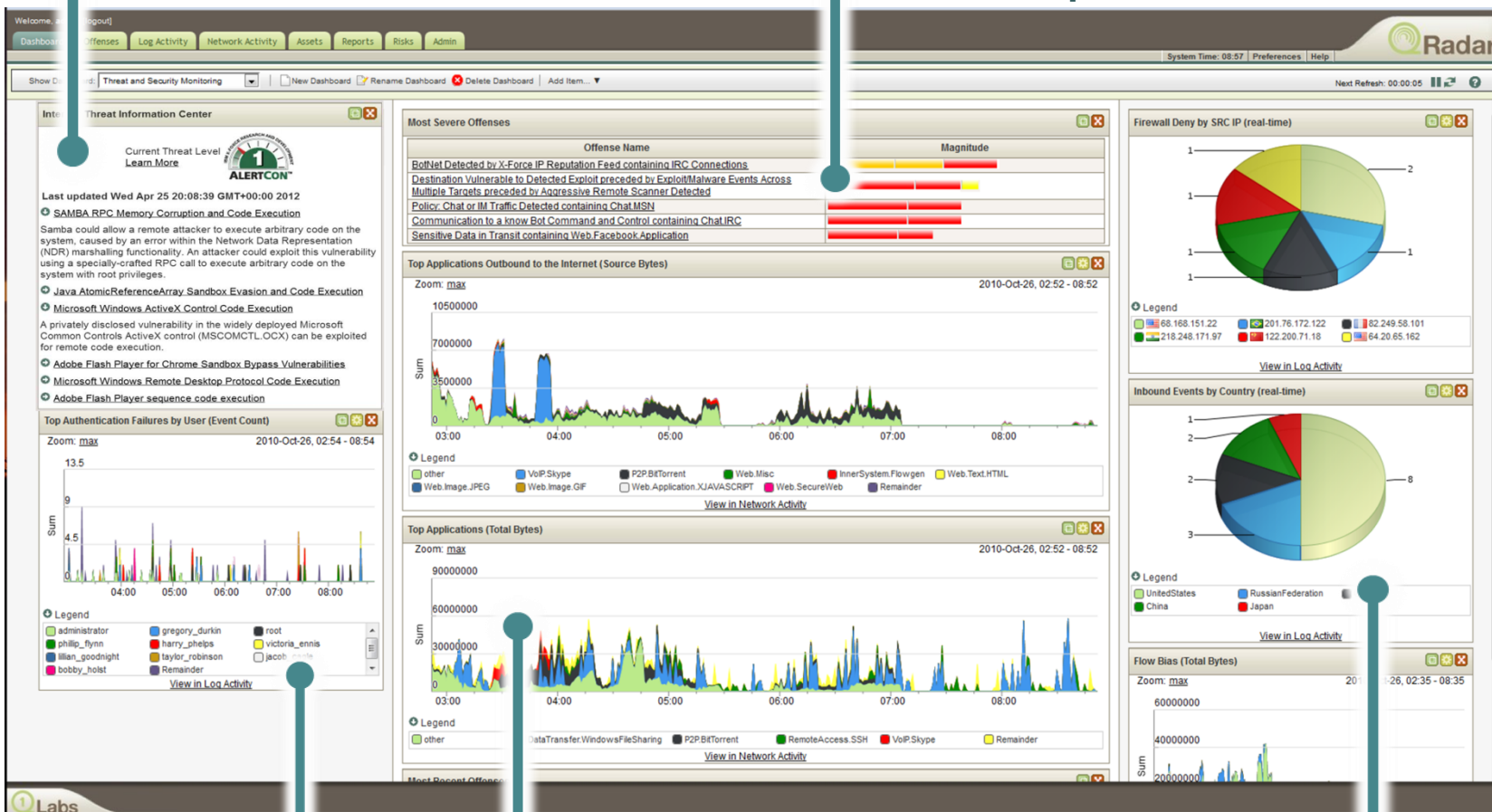
22,000 sensory
Organs on 22
appendages



QRadar provides security visibility and Security Intelligence

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation

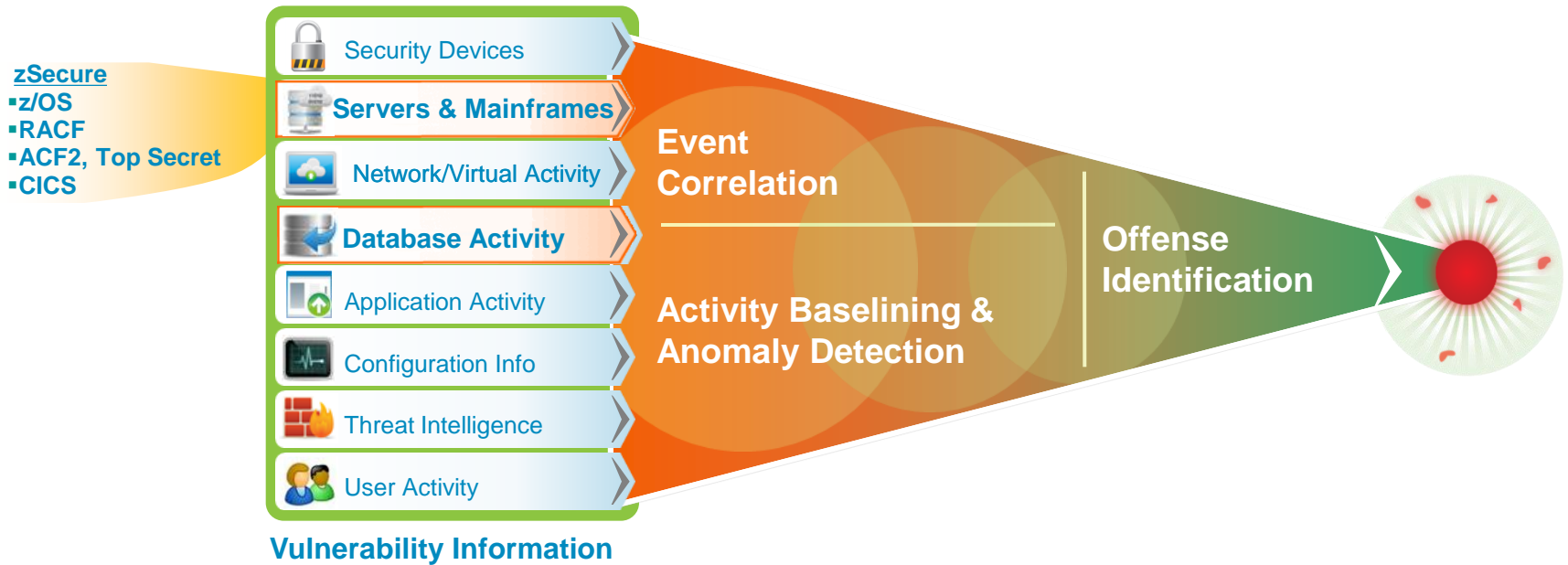


Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

zSecure and QRadar SIEM improve your Security Intelligence



Extensive Data Sources

+

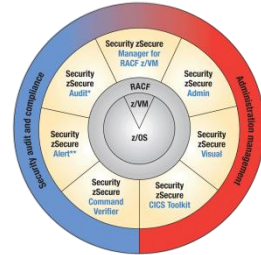
Deep Intelligence

=

Exceptionally Accurate and Actionable Insight

- ✓ Centralized view of mainframe and distributed network security incidents, activities and trends
- ✓ Better real-time threat identification and prioritization correlating vulnerabilities with zSecure
- ✓ SMF data set feeds with zSecure Audit and Alert
- ✓ Produces increase accuracy of risk levels and offense scores, and simplified compliance reporting

Enhanced security intelligence with integration with QRadar



■ Features

- Further maturation of the interfaces between Audit & Alert and QRadar SIEM
- Additional SMF fields made available in LEEF (Log Event Extended Format) files
 - LEEF files are the primary conduit for feeding events to QRadar SIEM
- New DB2 authorization field added to SMF and therefore available to LEEF files

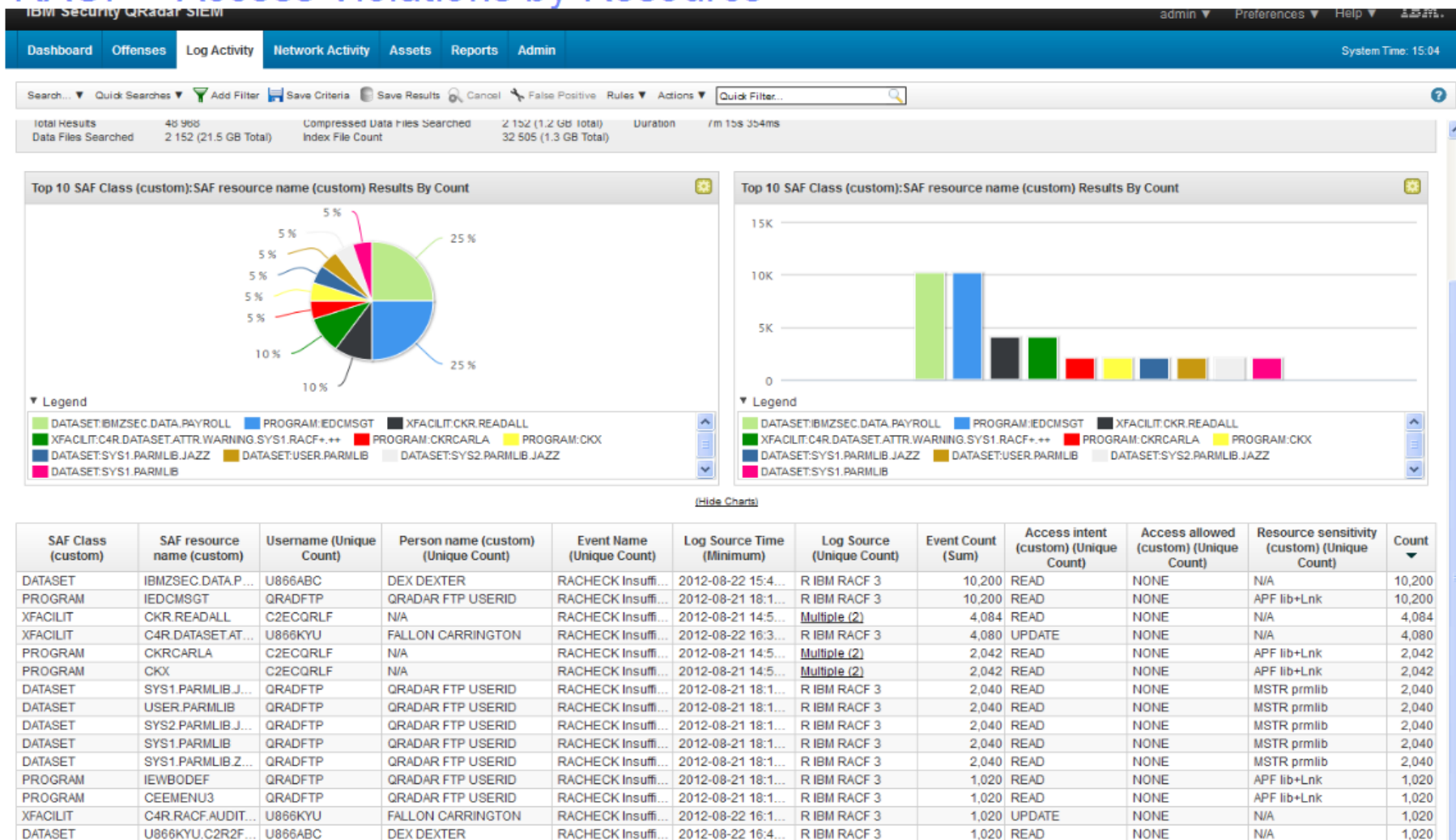
■ Benefits

- Richer set of z/OS data fed to QRadar means more intelligent analysis of security threats and therefore a more secure IT environment that includes z/OS
- CARLa enhanced for reporting – additional SMF fields made available





QRadar SIEM integration – RACF Sample


RACF – Access Violations by Resource



QRadar SIEM integration – Alert zoom in

Event Information	
Event Name:	Grant_Privilege_System
Low Level Category:	General Authentication Successful
Event Description:	System authority granted to user.
Magnitude:	
Username:	ROBVH
Start Time:	2013-02-21 18:02:49

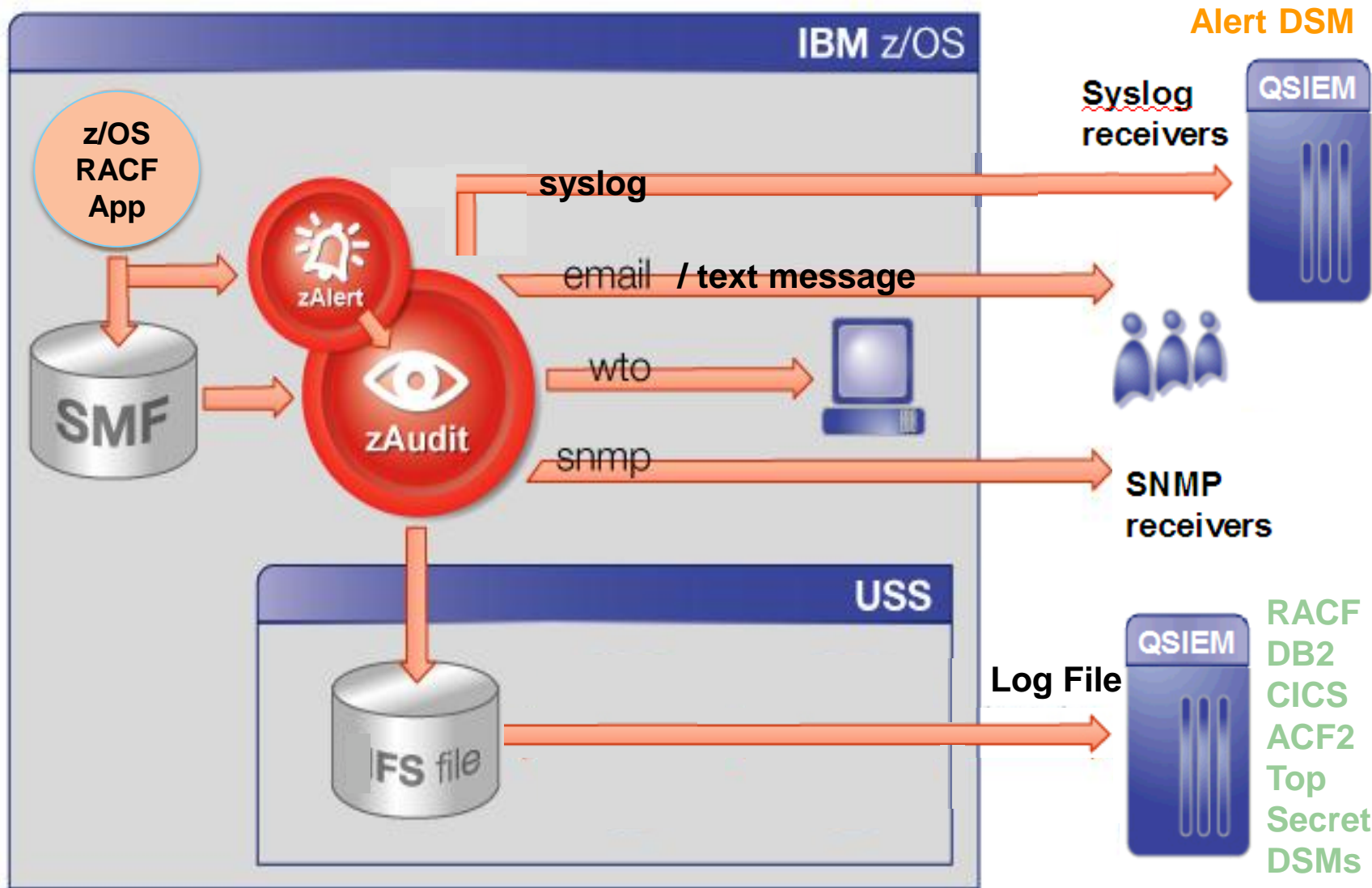
Event Information	
Event Name:	Change_APF_List_Added
Low Level Category:	Successful Configuration Modification
Event Description:	A data set is dynamically added to the APF list using SETPROG
Magnitude:	 (2)
Username:	N/A

Source and Destination Information	
Source IP:	 9.212.143.76
Source MAC:	00.00.00.00.00.00

Payload Information	
utf	hex base64
<input checked="" type="checkbox"/> Wrap Text	
<pre><117>Feb 21 17:03:48 ZT01 C2P1205 [C2P1205 onWhatDSNAME="PEASEJ.LOADLIB" whereSYSTEM="ZT01 "] Alert: Data set added to APF list using SETPROG: PEA</pre>	

Payload Information	
utf	hex base64
<input checked="" type="checkbox"/> Wrap Text	
<pre><117>Feb 21 18:00:50 ZT01 C2P1105 [C2P1105 onWhatAUTHORITY=" OPERATIONS AUDITOR" onWhatRACFCMD- whatACTION="Grant_Privilege_System" whatDESC="Success" whatRACFCMD="ALTUSER ROBVH3 AUDITOR OPER whereSYSTEM="ZT01"] Alert: System authority granted to ROBVH3 - System-level authority granted</pre>	

zSecure and QRadar SIEM – Architecture



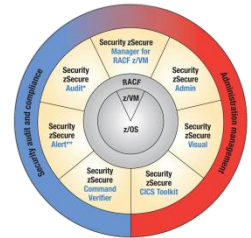
The Alert engine calls the Audit engine to format and send alerts

QRadar SIEM retrieves the LEEF files written by zSecure Audit into a z/OS UNIX directory

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
 - More...



* 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

Testing and reporting compliance

- Menu option **AU.R**
- Can select **more than one** standard, including site standard

```

Menu          Options          Info          Commands          Setup
-----
Command ==>  _____  zSecure Suite - Audit - Compliance
Compliance evaluation
■ STIG (subset)
_ GSD (subset)
_ Other standard member          _____
_ 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

```

Other zSecure 2.1 Enhancements

New for zSecure UI

- SMF reporting using IP address selection
- SMF reporting about SuperUser activity
- Support for Recreate of Universal Groups
- Extra selection when you really need to select on the complete absolute pathname
- Command Tailoring

zSecure Visual 2.1

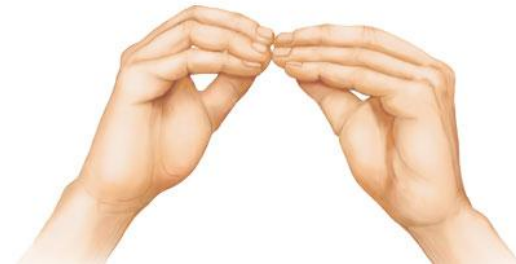
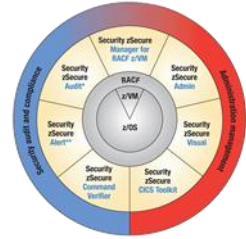
- Now provides support for site-specific REXX scripts

CARLa Enhancements

- Sort on look-up results instead of source
- Read DEFTYPE input from a file member
- Enhanced reporting on digital certificates
- New newlist showing information from ICSF TKDS tokens – 20 new fields and description
- New reporting capabilities for FTP and TELNET and support for new SMF subtypes and fields

Other Enhancements

- Enhanced compliance reporting of FTP and TN 3270
- Restrict access to RACF database via zSecure server
- Ease of multiple RACF system security administration



IBM Security zSecure SSE



Key solution highlights

- **Integrated mainframe security intelligence with Guardium Vulnerability Assessment**
 - provide zSecure RACF DB2 authorization information to Guardium VA for analysis.
 - coordinated GA date with Guardium VA 9.1
- **Support new DB2 V11 and IMS V13 releases**
 - coordinated GA date with DB2 V11 and IMS V13
- **Enhanced automated auditing & monitoring support for PCI DSS regulatory compliance**

Why IBM for Mainframe Security: Breadth, deep expertise, integration

Leadership

- Mainframes protect mission critical data and host up to 90% of mission-critical applications
- Enforce security best practices and compliance regulations such as PCI, HIPAA, worldwide regulations, and other privacy and industry standards
- Reduce cost and complexity of mainframe security:
 - Up to 70% in security audit savings
 - Up to 35% in reduced help desk calls
 - Up to 52% lower administrative costs

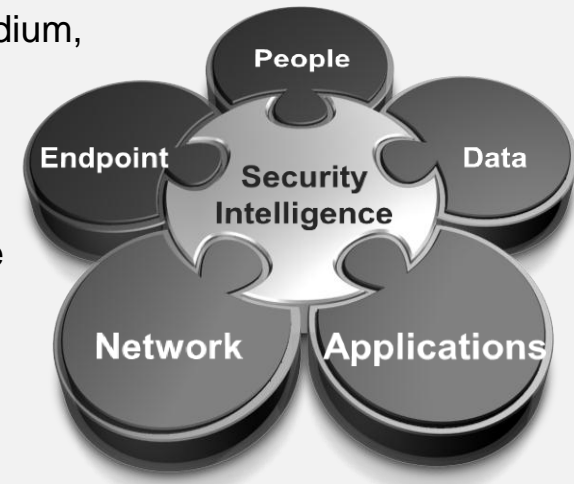
Integration

- Integration across the IBM Security portfolio including zSecure Guardium, Security Identity and Access Management, RACF, and IBM Security Key Lifecycle Manager for security intelligence
- Integration and audit reporting for z/OS, UNIX, Linux on System z, DB2, CICS, IMS, WebSphere® Application Server, OMEGAMON® XE on z/OS, HSM, Communication Server, TCP/IP, PDSE and more

Expertise

- Worldwide security research centers and security operations centers

Think Integrated.





ibm.com/security

© **Copyright IBM Corporation 2013. 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.