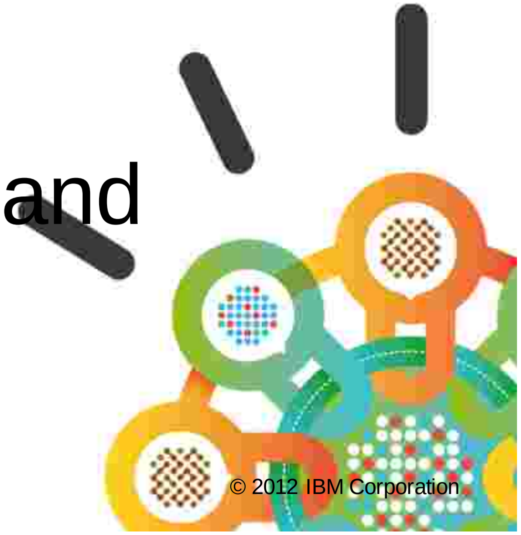
zSecure Suite 2.1 Beta Release Customer Experience

Demonstrating Governance, Risk and Compliance on your Mainframe



Trademark

Trademark

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

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

* 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.

2

Session Abstract

- zSecure 2.1 (Beta) provides new audit and compliance capabilities; establishes integration with QRadar; and exploits new z/OS 2.1 operating system features. The Customer presenter will speak on how the new features enabled improved security and compliance management; event monitoring and reporting; and other benefits to improve automation and further reduce costs.

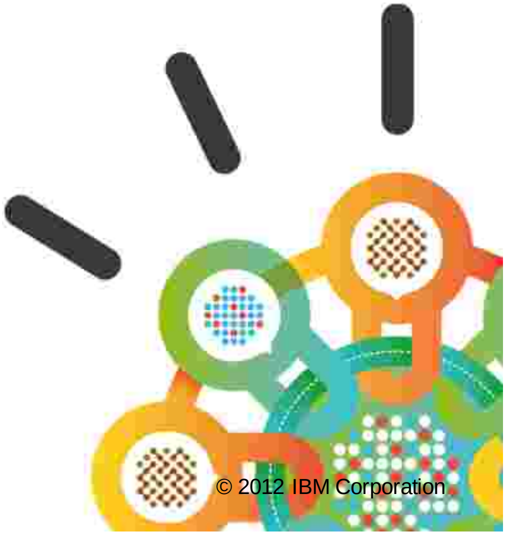
Agenda

- Release announcement
- Beta background
- Customers
- Customer Experiences
- Questions

zSecure suite 2.1

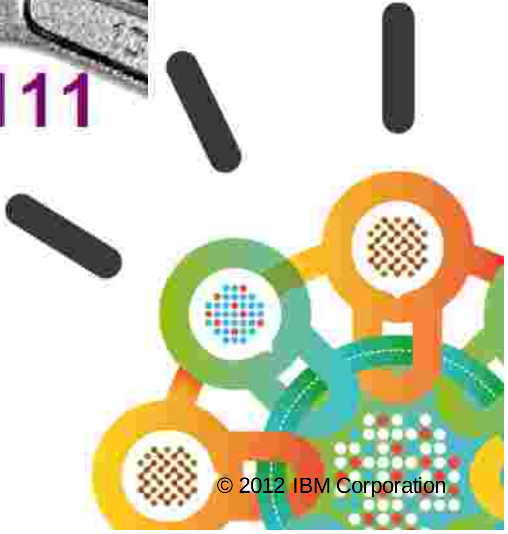
§Announced July 23 with z/OS and RACF 2.1

§GA September , 2013



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

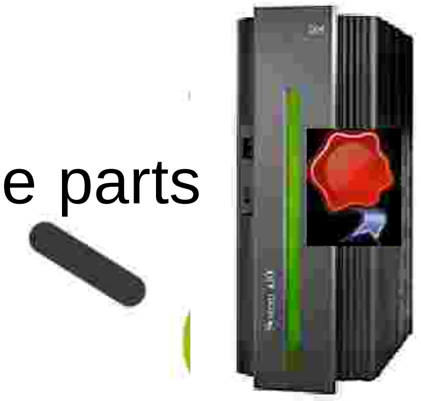
- Features
  - Collect data from additional DB2 object types, primarily related to access levels
  - Collect data from DB2 Internal Access Control Lists to track effective access
  - Collect data on potential conflicts between DB2 Internal Access Control Lists and RACF
- Benefits
  - More effective audit of database access improves integrity of DB2 databases
  - Reduces requirements for manual audits of DB2 access therefore reduction in personnel resource requirements

RACF Digital Certificate Management

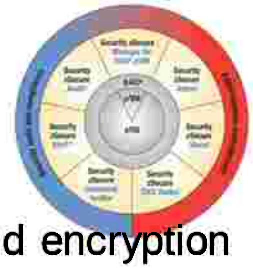
ISSUES:

- Difficult to find what to do where
  - Solution: Totally redesigned user interface for certificates

    New menus and new line commands
- Error prone, difficult to remember all certificate parameters
  - Solution: introduce certificate templates
- Difficult to remember TKDS token names to use on BIND
  - Solution: display selection list of token names
  - TKDS information is obtained via CKFREEZE
- Difficult to find or sort on Distinguished Name parts
  - Solution: Added function to extract Distinguished Name parts



Enhanced support for administration of RACF digital certificates

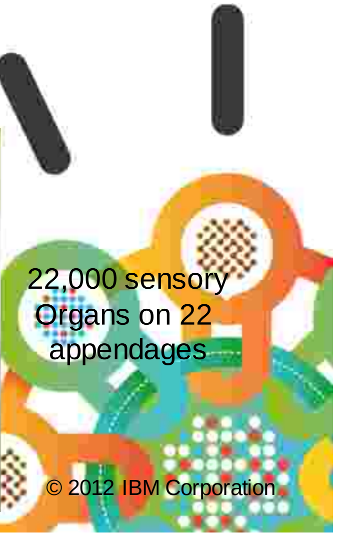


- RACF Digital Certificates
  - Digital Certificates are used for enhance authentication, verification, and encryption
  - RACF supports digital certificates for use with z/OS
- Features
  - New facility to create, administer, customize and audit RACF digital certificates
  - New Facility to create certificate 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)



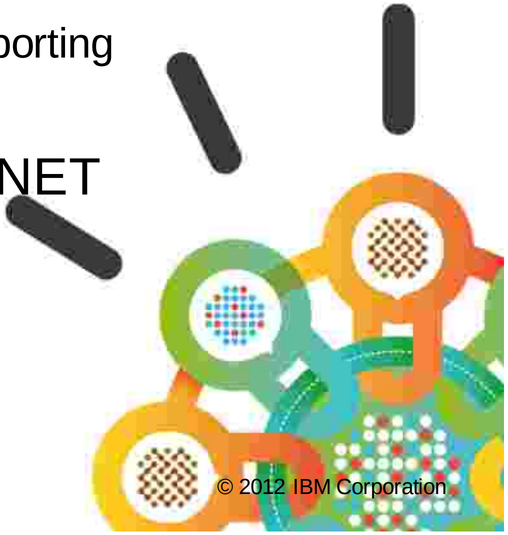
22,000 sensory Organs on 22 appendages

Problems with compliance testing in the past

- Built-in standards (C1 / C2 / B1) are considered to be 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 create 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.

Compliance Testing Framework

- Support newer external standards
  - DISA STIG for z/OS RACF
  - DISA STIG for z/OS ACF2
  - IBM outsourcing GSD331/iSec
- Eliminate need for 2-pass queries
- Show positive compliance, not just non-compliance
- Allow showing progress in compliance efforts
- Support in-standard customization
  - Members with authorized 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, IP, FTP, TELNET

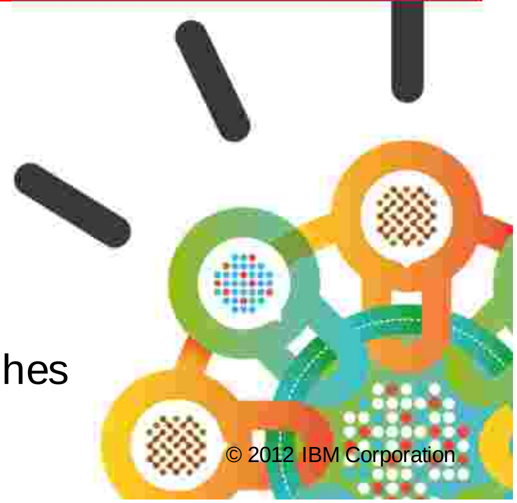


Enhanced compliance reporting

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

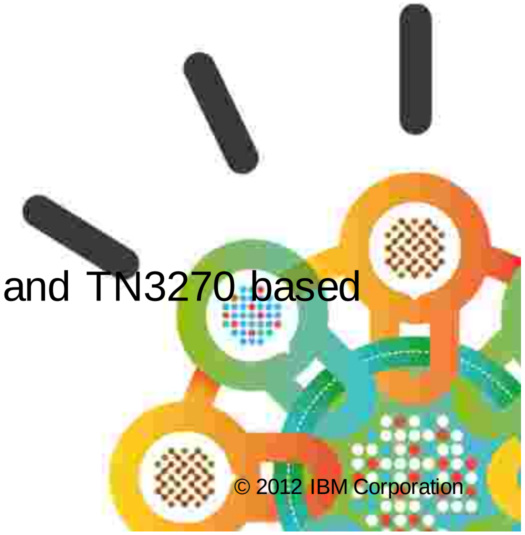
* STIG: Security Technical Implementation Guide; Guidelines from US Defense Information Systems Agency (DISA)

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



Enhanced compliance reporting of FTP and TN3270

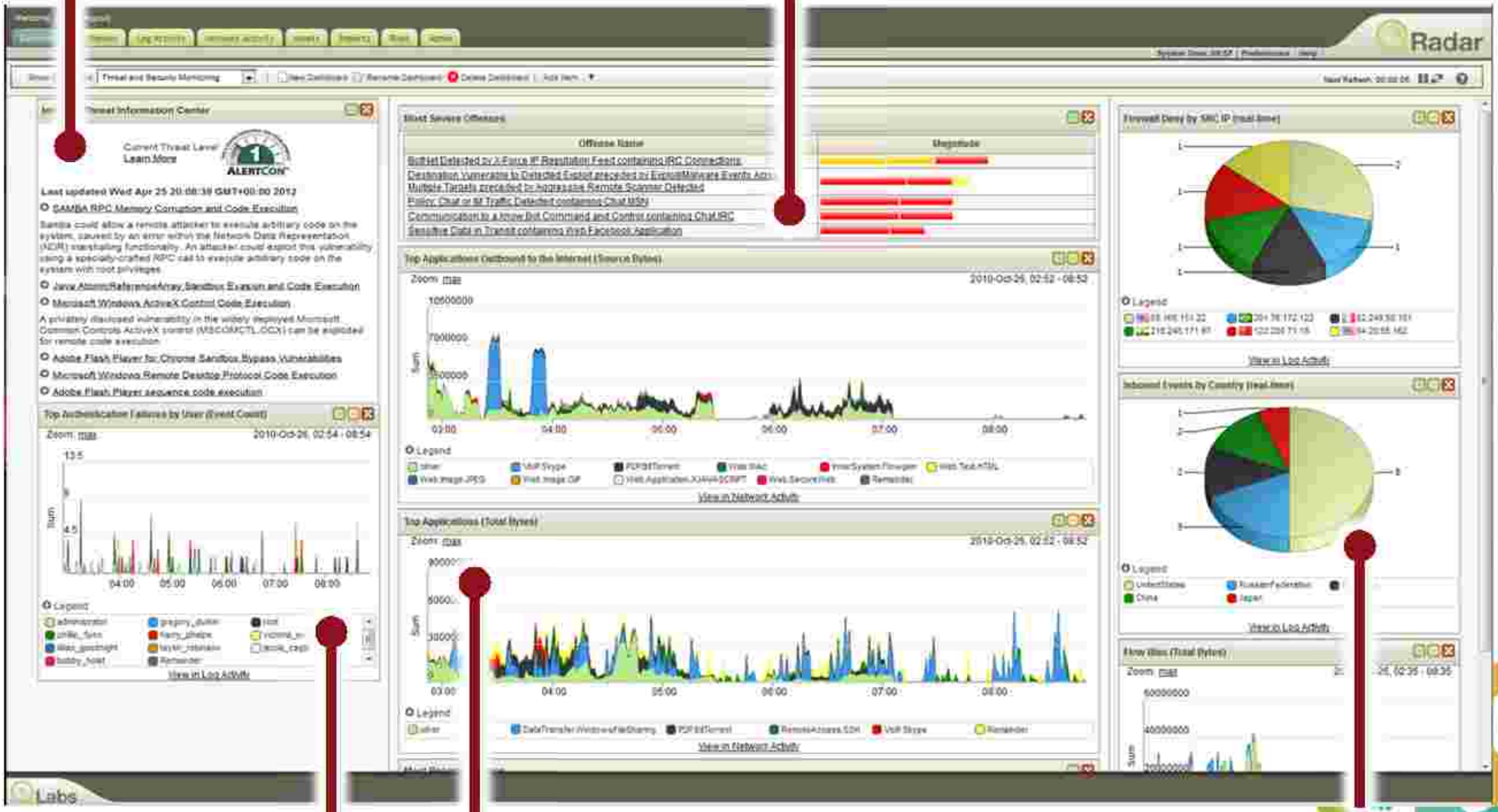
- What is FTP and TN3270
  - z/OS FTP provides for file transfers between z/OS and other systems
  - TN3270 (Telnet 3270) emulates the text based interactions of legacy IBM terminals that were utilized pre-PC
- Features
  - New API in Communication Server exploited by zSecure to capture communication settings
  - Extended SMF logging by Communications Server exploited by zSecure to audit FTP and TN3270 streams
  - Reporting FTP Daemon configuration changes - SMF
- Benefits
  - Extends benefits of zSecure Audit to these legacy applications
  - Address compliance requirements of PCI-DSS and STIG for FTP and TN3270 based applications



QRadar provides security visibility and Security Intelligence

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



Threat Information Center

Current Threat Level
Learn More

Last updated Wed Apr 25 20:08:39 GMT+00:00 2012

○ SAMBA RPC Memory Corruption and Code Execution

Samba could allow a remote attacker to execute arbitrary code on the system, caused by an error within the Network Data Representation (NDR) marshalling functionality. An attacker could exploit this vulnerability using a specially-crafted RPC call to execute arbitrary code on the system with root privileges.

○ Java AtomicReferenceArray Sandbox Evasion and Code Execution

○ Microsoft Windows ActiveX Control Code Execution

A privately disclosed vulnerability in the widely deployed Microsoft Common Controls ActiveX control (MSCOMCTL.OCX) can be exploited for remote code execution.

○ Adobe Flash Player for Chrome Sandbox Bypass Vulnerabilities

○ Microsoft Windows Remote Desktop Protocol Code Execution

○ Adobe Flash Player sequence code execution

Most Severe Offenses

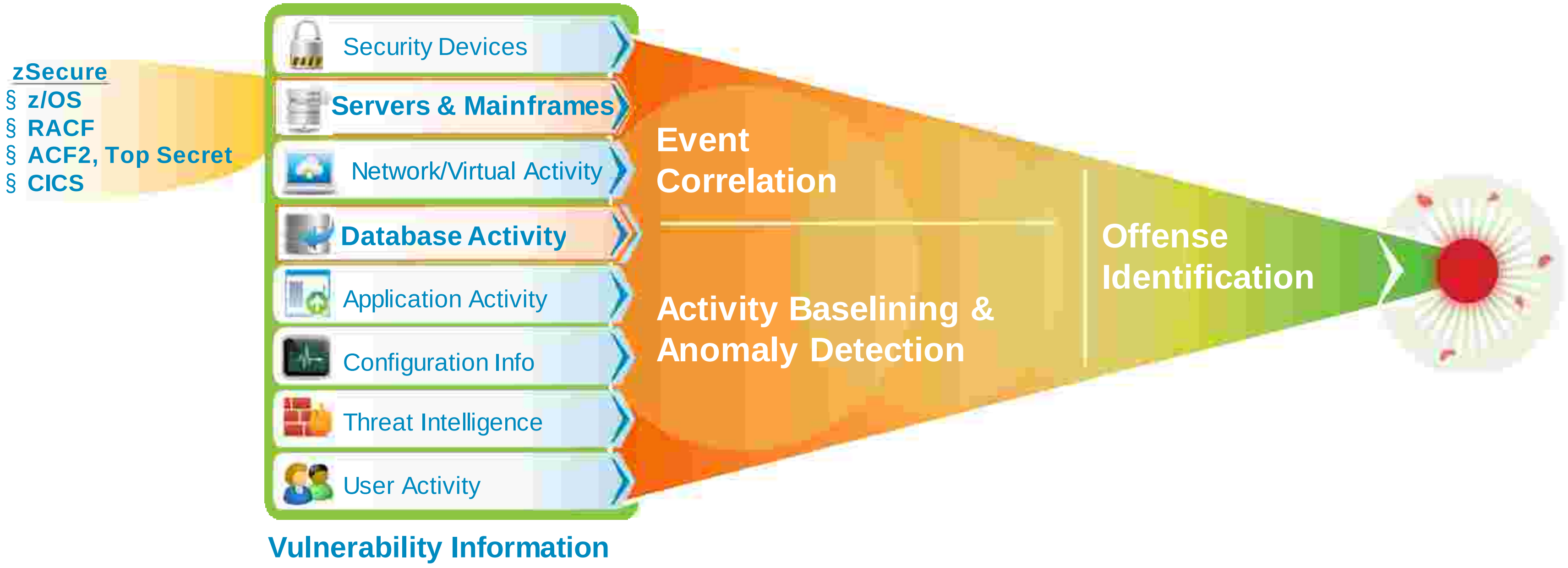
Offense Name	Magnitude
BotNet Detected by X-Force IP Reputation Feed containing IRC Connections	
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Acr	
Multiple Targets preceded by Aggressive Remote Scanner Detected	
Policy: Chat or IM Traffic Detected containing Chat MSN	
Communication to a know Bot Command and Control containing Chat IRC	
Sensitive Data in Transit containing Web Facebook Application	

Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

zSecure and QRadar improve your Security Intelligence



zSecure
- § z/OS
- § RACF
- § ACF2, Top Secret
- § CICS

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

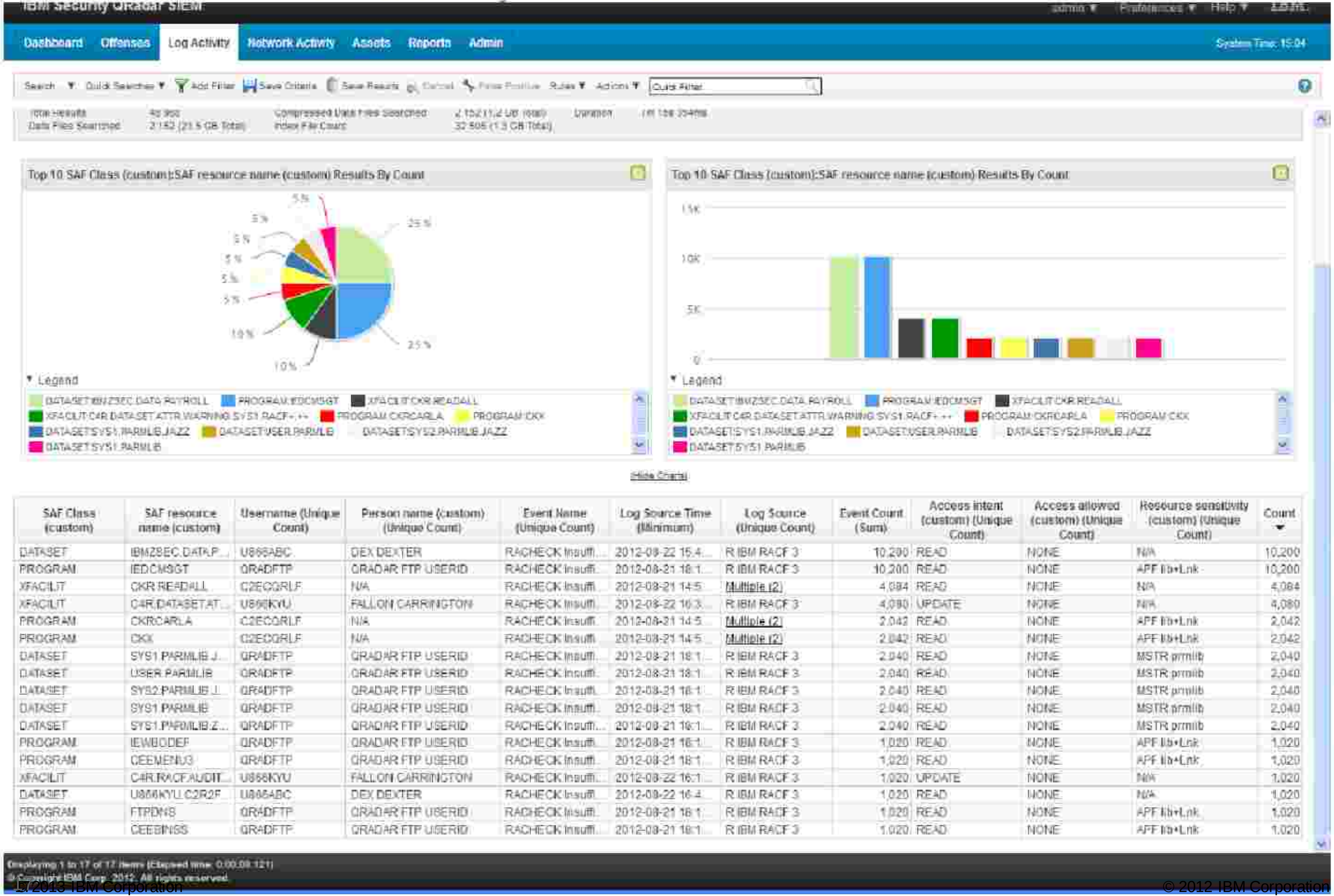
ü Centralized view of mainframe and distributed network security incidents, activities and trends

ü Better real-time threat identification and prioritization correlating vulnerabilities with zSecure

ü SMF data set feeds with zSecure Audit and Alert

ü Produces increase accuracy of risk levels and offense scores, and simplified compliance reporting

RACF – Access Violations by Resource



Total Results 45,950 | Data Files Searched 2,152 (21.5 GB Total) | Compressed Data Files Searched 2,152 (1.2 GB Total) | Index File Count 32,505 (1.3 GB Total) | Duration 1m 18s 254ms

SAF Class (custom)	SAF resource name (custom)	Username (Unique Count)	Person name (custom) (Unique Count)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Event Count (Sum)	Access intent (custom) (Unique Count)	Access allowed (custom) (Unique Count)	Resource sensitivity (custom) (Unique Count)	Count ▼
DATASET	IBMZSEC.DATA.P...	U866ABC	DEX DEXTER	RACHECK Insuffi...	2012-08-22 15:4...	R IBM RACF 3	10,200	READ	NONE	N/A	10,200
PROGRAM	IEDCMSGT	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	10,200	READ	NONE	APF lib+Lnk	10,200
XFACILIT	CKR.READALL	C2ECQRLF	N/A	RACHECK Insuffi...	2012-08-21 14:5...	Multiple (2)	4,084	READ	NONE	N/A	4,084
XFACILIT	C4R.DATASET.AT...	U866KYU	FALLON CARRINGTON	RACHECK Insuffi...	2012-08-22 16:3...	R IBM RACF 3	4,080	UPDATE	NONE	N/A	4,080
PROGRAM	CKRCARLA	C2ECQRLF	N/A	RACHECK Insuffi...	2012-08-21 14:5...	Multiple (2)	2,042	READ	NONE	APF lib+Lnk	2,042
PROGRAM	CKX	C2ECQRLF	N/A	RACHECK Insuffi...	2012-08-21 14:5...	Multiple (2)	2,042	READ	NONE	APF lib+Lnk	2,042
DATASET	SYS1.PARMLIB.J...	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	USER.PARMLIB	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	SYS2.PARMLIB.J...	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	SYS1.PARMLIB	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	SYS1.PARMLIB.Z...	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
PROGRAM	IEWBODEF	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020
PROGRAM	CEEMENU3	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020
XFACILIT	C4R.RACF.AUDIT...	U866KYU	FALLON CARRINGTON	RACHECK Insuffi...	2012-08-22 16:1...	R IBM RACF 3	1,020	UPDATE	NONE	N/A	1,020
DATASET	U866KYU.C2R2F...	U866ABC	DEX DEXTER	RACHECK Insuffi...	2012-08-22 16:4...	R IBM RACF 3	1,020	READ	NONE	N/A	1,020
PROGRAM	FTPDNS	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020
PROGRAM	CEEBINSS	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020

Displaying 1 to 17 of 17 items (Elapsed time: 0:00:00.121)

Other zSecure 2.1 Enhancements

- New for zSecure UI
  - – SMF reporting using IP address selection

§ USS extended support

- 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

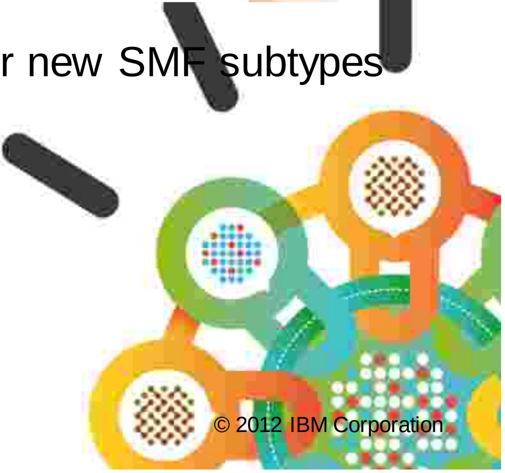
- Now provides support for site-specific REXX scripts

§ CARLa Enhancements

- 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

§ Restrict access to RACF database via zSecure server

§ Other Enhancements



Agenda

- Release announcement
- Beta background
- Customers
- Customer Experiences
- Questions

Beta Participant Benefits

- **The Beta participants experience the following benefits:**
  - The opportunity to discuss problems and share ideas with product experts from IBM and with other customers, via web conferences and an online web-based Discussion Forum.
  - The ability to install, configure and/or evaluate the new product code in their own test environment to validate new functionality and ensure the product works in their environment before the product goes GA.
  - Dedicated support provided by Development for the duration of the beta program, via an online web-based Discussion Forum.
  - An opportunity to influence the product function and future directions.
  - For those new customers who do not currently have zSecure it is a great opportunity for them to try it out during the beta program.

What IBM Expects from Beta Participants

- **What do we expect from the beta participants?**
  - Download the beta code drops and install them
  - Test out the functions that are important to you and post any problems and questions to an online web-based Discussion Forum
  - Provide occasional status by submitting an online Feedback form when requested by us
  - Consider being a reference at the end of the beta program if your company has a positive experience

Agenda

- Release announcement
- Beta background
- Customers
- Customer Experiences
- Questions

Customers

- **Customer in Beta for zSecure 2.1**
  - Government (multiple
  - Health Care (multiple)
  - Automotive
  - Finance (multiple)
- Reasons
  - Need to expand auditing capabilities
  - Want to use digital certificates but find them difficult
  - Needed to be able to audit DB2 more than just what was in RACF database (if it was even in the RACF database)
  - Beta customer for z/OS 2.1
  - Interested in enhancements to zSecure Admin Access Monitor
  - STIG and GSD331, improve PCI DSS efforts

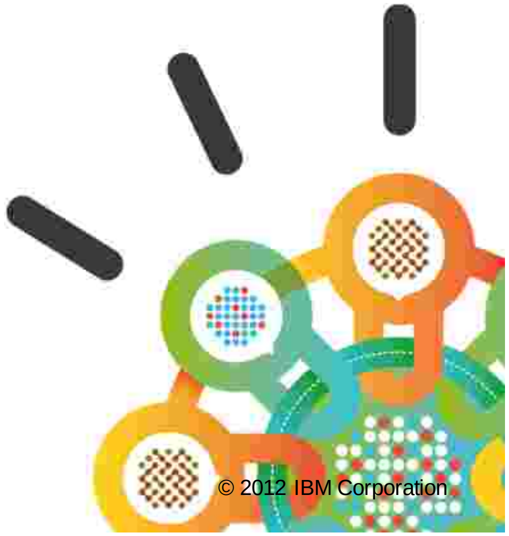
Agenda

- Release announcement
- Beta background
- Customers
- Customer Experiences
- Questions

Customers Experiences

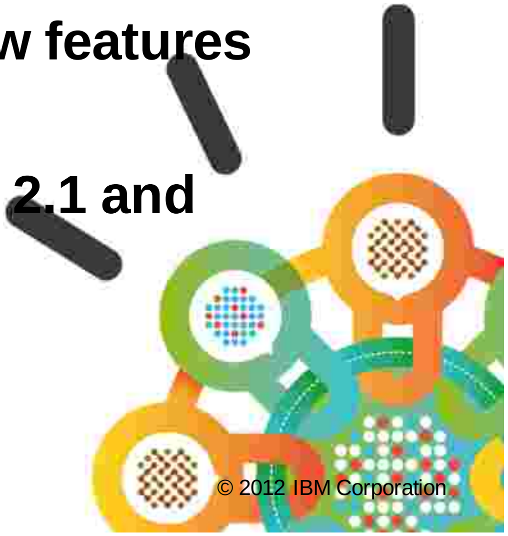
- **Customer Experiences – Some of the key areas tested**
  - Compliance
  - Digital Certificates
  - Access Monitor
  - DB2
  - TCP/IP reporting

- Customer present -- Mark Wilson – RSM Partners – Beta Customer



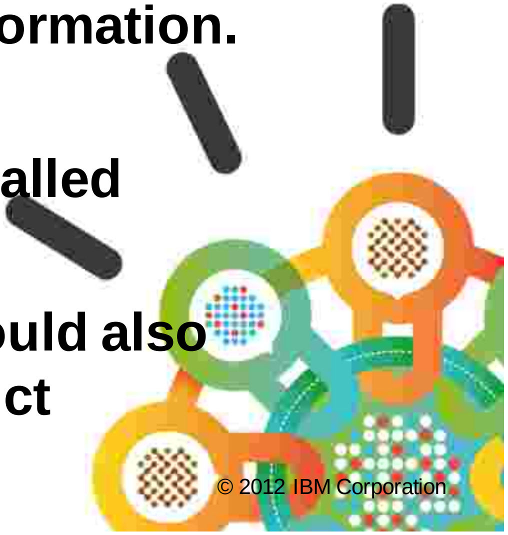
Customers Experiences

- Customer Feedback
  - Will do it again
  - Digital certificates WOW!!, this helps so much. I always had to get tech support involved.
  - Was able to provide feedback on how I wanted the product to display information
  - Training sessions – great to get trained on the new features
  - Good to know what was also coming out in RACF 2.1 and z/OS that zSecure would support
  - Great interfacing with development



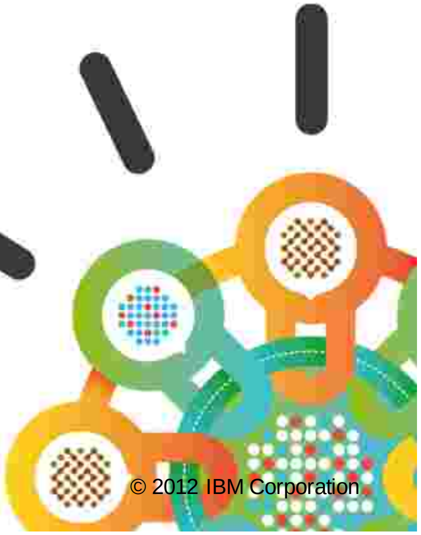
Customers Experiences

- **Customer Feedback**
  - **Wow, I was able to influence some areas of the product (e.g., display, help text, reporting)**
  - **Easy to provide feedback**
  - **Response time was quick (not what I expected at all)**
  - **Web sessions were great – the interaction was great. Being able to ask questions right there and get more information.**
  - **Was easy to get the product downloaded and installed**
  - **Forum provided a lot of great information and I could also see what other people had to say about the product**



Customers Experiences

- **Customer Feedback**
  - **I was getting so bogged down in compliance reporting this is a tremendous help. It will save a lot of time.**
  - **Access Monitor keeps getting better and better. It was good before, I am using it of other thing other that intended purposes. New features will help even more**
  - **I am trying to externalize DB2 security this release will continue to assist me with that migration**
  - **I don’t have a strong network background, the new features continue to make it easier for me to learn and look for exposures.**



Questions

ibm.com/security