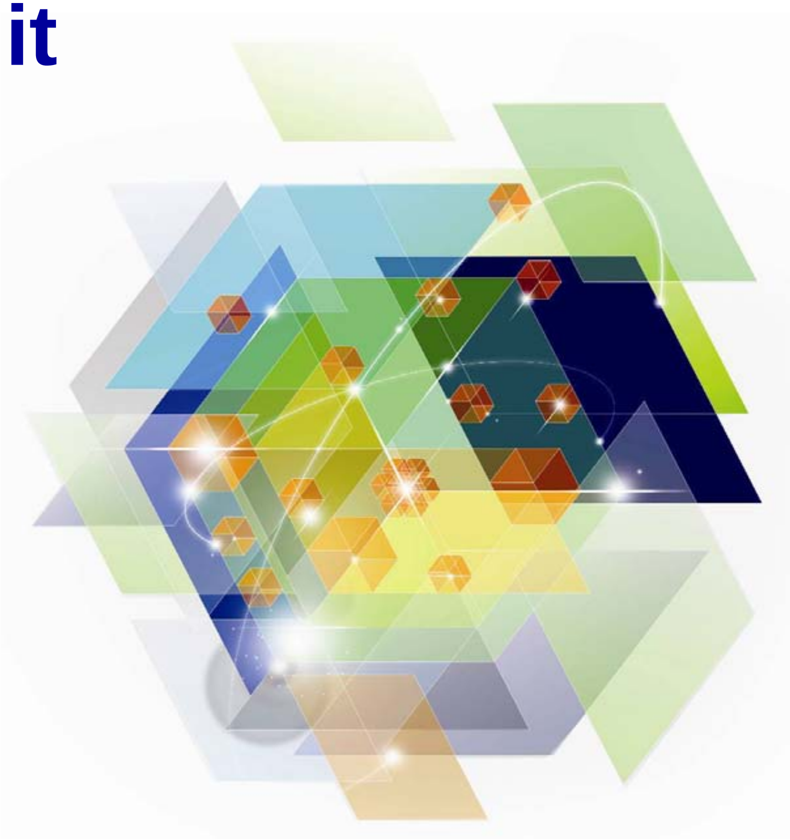
Security Intelligence, Audit and Compliance



Agenda

Concerns

Actions

Is the Mainframe Vulnerable?

- **Hacking/Theft (just to mention a few)**
  - – Department store mainframe security hack
  - – Health care mainframe security hack
  - – Mainframe computer physically lost from college campus
  - – Airport mainframe computer physically moved
- **Insider Threat?**
  - – Long considered the most serious threat
    - Insiders have access
    - Insiders have knowledge
    - Insiders have economic motivation
    - Insider collusion is a “force multiplier”

Mainframe security

What's the risk?

– Disclosure of sensitive data
– Service interruption
– Corruption of operational data
– Fraud and ID Theft
– Theft of services

What's at stake?

- Customer trust
- Reputation and Brand
- Privacy
- Integrity of Information
- Legal and Regulatory Action
- Competitive Advantage

Breach cost?

$ Research and recovery
$ Notify customers
$ Lost customer business
$ Problem remediation
$ Claims from trusted vendors and business partners

$$ Damage to brand image

Mainframe Vulnerabilities

Mainframe Security Report 1:

Security Officer Representation: We restrictively secure our mainframe based-on the concept of “least privilege”. Nobody gets access to anything unless it is approved.

Report Finding: The mainframe security and the protection-by-default mechanisms of the mainframe security software have been promiscuously configured to the point of providing access by default instead of protection. The security of system and application resources cannot be assured.

Reality of security contradicts perception

Mainframe Vulnerabilities

Mainframe Security Report 2:

Security Officer Representation: It is our practice to empower business units to make decisions regarding the security of their applications and services.

Report Finding: As authorized by a business unit, CICS regions were running with full security bypass privilege, leaving CICS technical resources and the data of all applications vulnerable to system programmers, CICS sub-system programmers, and application programmers. Result: No separation of function between applications; no assurance of data privacy protection; no assurance of production operation.

No Security Implementation Standards

a.ka. “Adult Supervision”

Mainframe Vulnerabilities

Mainframe Security Report 3:

Mainframe security is being managed and administered using legacy practices and standards that pre-date the increased technical sophistication of the mainframe and its increased leverage for Web-based services. As such, security is woefully inadequate to assure security , privacy, and compliance in the current environment.

Mainframe is Dead Legacy…

Low investment, weak skills, weak governance, maybe coupled with a false sense that the mainframe is inherently secure

Story of a Security Consultant

Unix System Services Hack

Due to the regular mis-configuration of security in the z Unix System Services environment and inappropriate use of security bypass privileges, one security practitioner has repeatedly demonstrated the ability to compromise mainframe security and grab any data desired.

His record hack time: Less than 20 minutes!!!

One of the successes was by invitation against a security software company.

Advice From a Career Auditor

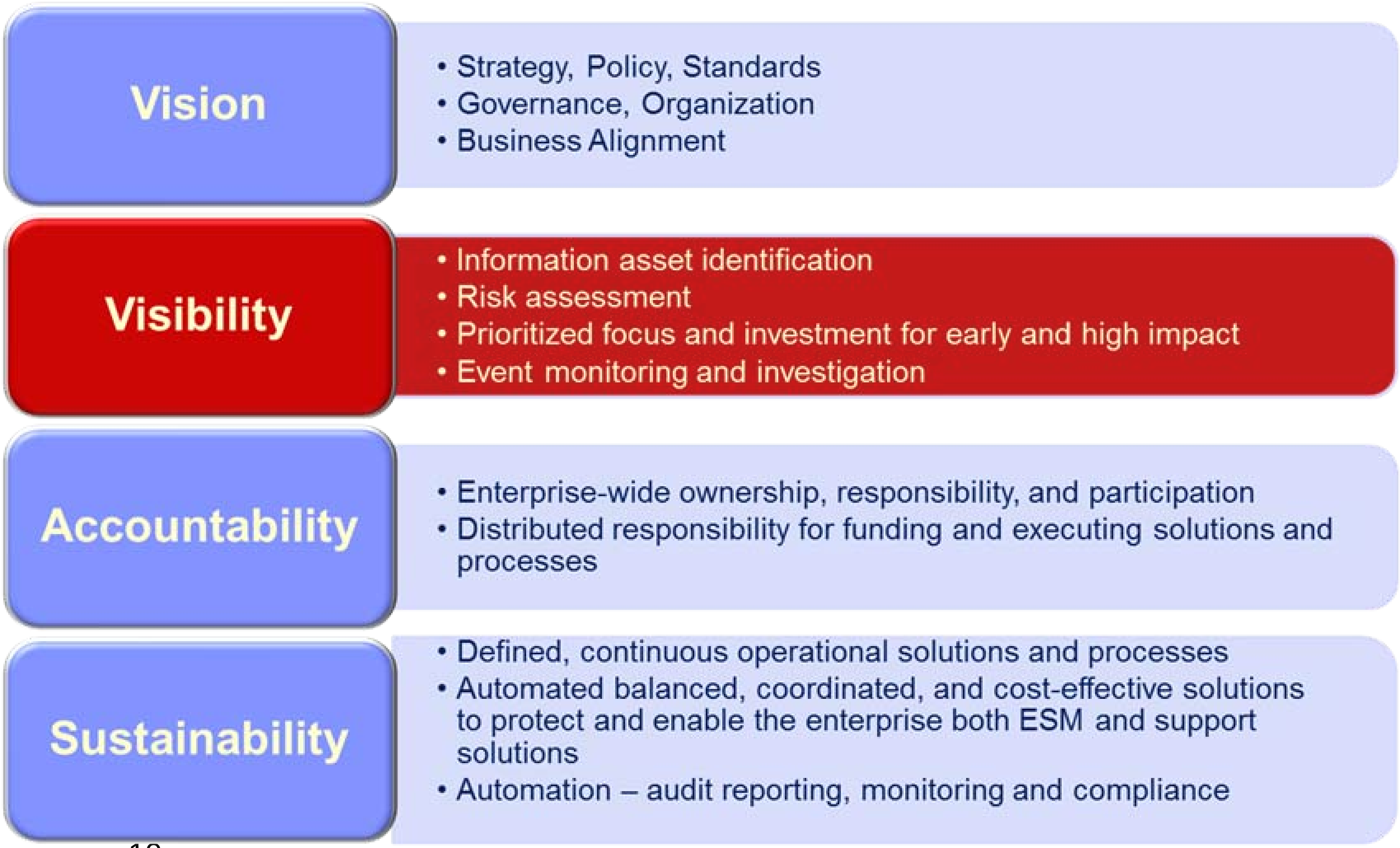
"You don't know what you don't know, and what you don't know will hurt…!"

Senior Manager ,
U.S. Government Accountability Office

SHARE 2012 Atlanta

SEC Project Keynote Presentation

Information Security Optimization Principles



Vision	• Strategy, Policy, Standards • Governance, Organization • Business Alignment
Visibility	• Information asset identification • Risk assessment • Prioritized focus and investment for early and high impact • Event monitoring and investigation
Accountability	• Enterprise-wide ownership, responsibility, and participation • Distributed responsibility for funding and executing solutions and processes
Sustainability	• Defined, continuous operational solutions and processes • Automated balanced, coordinated, and cost-effective solutions to protect and enable the enterprise both ESM and support solutions • Automation – audit reporting, monitoring and compliance

Advice From a Career Information Security Consultant

**“If nobody is minding the store,
someone will surely steal the goods”**

Quote from *Security Consultant from TATA America International Corporation*

The one thing you can do to immediately strengthen security without risking unintended denials of access is to initiate aggressive monitoring and investigation.

What you see will surprise you! The visibility will convince you! The implications will motivate you.

Obtain Security Intelligence: You need to determine what you don’t know before you can do anything meaningful!

A Final Keystone Issue

Relative to the Information Security trilogy of Confidentiality, Integrity, and Availability, legacy mainframe security implementations consistently exhibit a strong bias to Availability, at the expense of Confidentiality and Integrity.

A Final Keystone Issue: Balance Required

C I A

Balance is needed across C, I, and A to assure effective security. Lack of balance results in exposures and vulnerabilities

Your Conflict: Regulation versus Reality

Regulation

- **Change management**
  - Clearly defined process with approval and reporting
  - Ability to identify changes
- **Security management**
  - Separation of duties
  - Identification of exposures and mis-configurations
  - Clear audit trail and accountability
- **Data security**
  - Data confidentiality and integrity
  - Prevent improper access to financial, medical or personal data
  - Monitor access to data by technician, administrator, outsiders

Reality

- **Separation of duty impractical tasks with small teams**
- **Many highly authorized IDs necessary for final go-to technician**
- **Mainframe installations often rely on “system special” and “uid(0)”**
- **Red-tape bypassed for high-impact problem resolution**
- **Manual monitoring impractical**
  due to volume of data
- **Human mistakes cause service outages**
- **Cleanup projects are long running and expensive**

Concerns

Actions

Take Charge

- **As you move into the action phase**
  - You need to take the lead to set the foundations
  - Prepare and obtain top level management support for a foundational Security Implementation & Administration Policies document (when was the last time these were reviewed)
  - Actions must be based upon what you see and what needs to be controlled as defined by your policies that support the business compliance and risk
  - What do you look for and how do you move towards the target state of control and compliance?
  - What do you have in the way of software that can help or what do you need?
  - **Automate** the review and enforcement of controls both existing and those established during this ongoing process

Common IT General Control Deficiencies

Excessive Access to Systems / Databases

- Developer / programmer access to production environment
- Developer / programmer access to production data
- DBA access
- System Administrator access

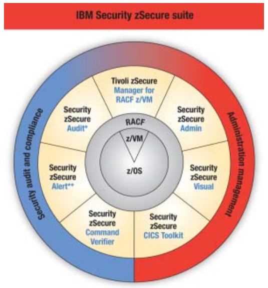
Lack of Access Controls

- User provisioning and administration
  - Changes in responsibilities
  - Changes in organization
  - Terminations
- No documented access policies and standards

Lack of General monitoring of the security infrastructure

Technology can help

- **Define the security policy in monitoring tools**
  - Operating system and security settings against baselines
  - Operating system and security changes against baselines
  - Data access against standards
  - Access by technicians should fit production profile
  - etc.
- **In case of conflict**
  - Deny the action, prevent the change from taking place, or
  - Issue a real-time message to data security officer, or
  - Generate an exception report for review by management
- **Document**
  - Baseline or security standard
  - Exceptions and transgressions


IBM Security zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Introducing QRadar: From head of IT security at a North American Bank

The head of IT security at a bank moved to a new bank and reported on the first month security situation.

“I haven’t seen any evidence of sophisticated attack attempts against the bank within the past month.”

Her supervisor thought that was very good news, and that the bank must be protected.

“No, it’s not good. Other banks like ours are tracking several sophisticated attempts each week. Here I don’t see any of that information but I know they must be occurring.”

Customer Challenges

Detecting threats

- Arm yourself with comprehensive security intelligence

Consolidating data silos

- Collect, correlate and report on data in one integrated solution

Detecting insider fraud

- Next-generation SIEM with identity correlation

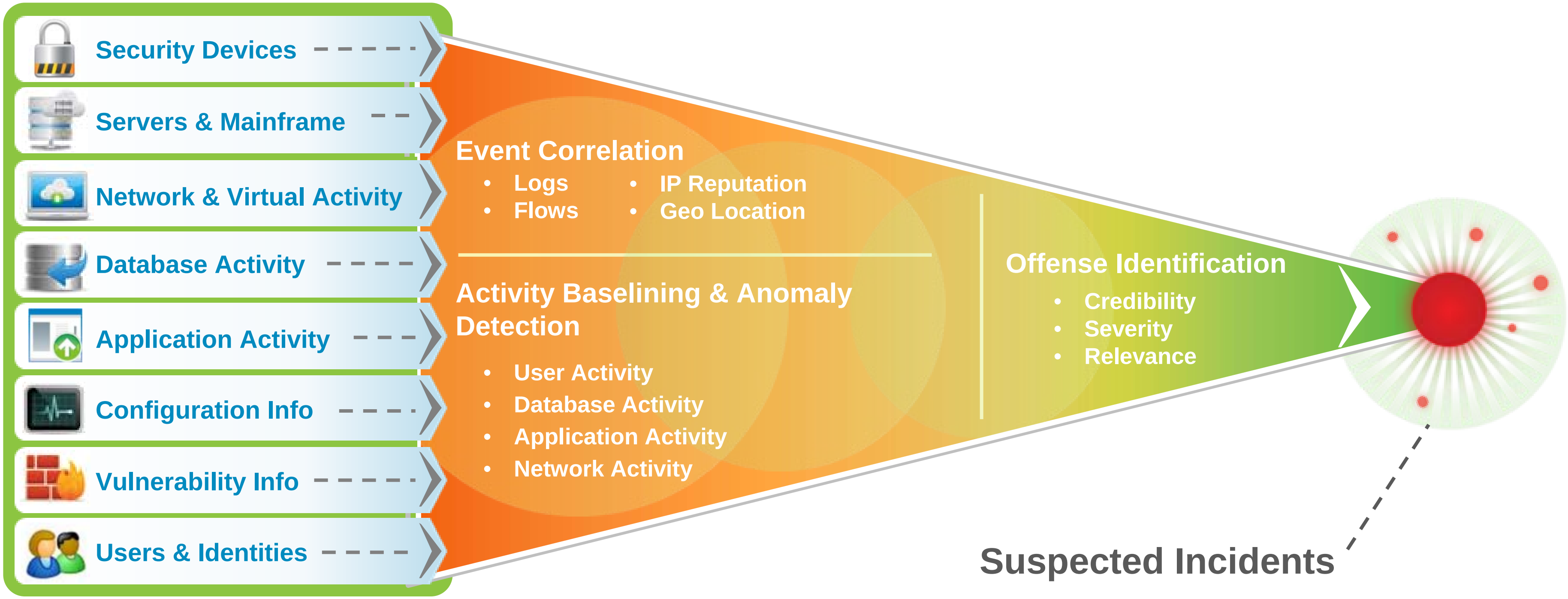
Better predicting risks to your business

- Full life cycle of compliance and risk management for network and security infrastructures

Addressing regulation mandates

- Automated data collection and configuration audits

Context and Correlation Drive Deep Insight and Accurate Detection



- Security Devices
- Servers & Mainframe
- Network & Virtual Activity
- Database Activity
- Application Activity
- Configuration Info
- Vulnerability Info
- Users & Identities

Event Correlation

- Logs
- Flows
- IP Reputation
- Geo Location

Activity Baselining & Anomaly Detection

- User Activity
- Database Activity
- Application Activity
- Network Activity

Offense Identification

- Credibility
- Severity
- Relevance

Suspected Incidents

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

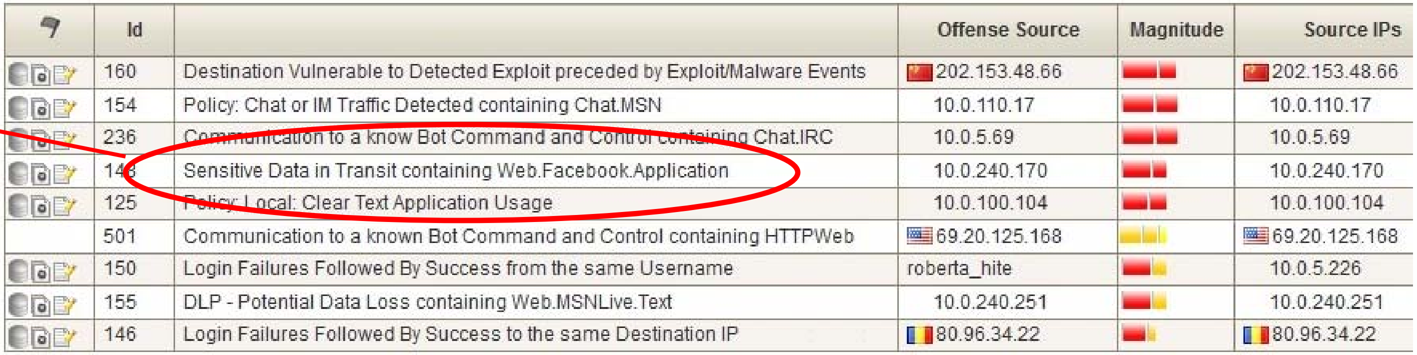
Solving Customer Challenges

Major Electric Utility	Detecting threats	• Discovered 500 hosts with "Here You Have" virus, which other solutions missed
Fortune 5 Energy Company	Consolidating data silos	• 2 Billion logs and events per day reduced to 25 high priority offenses
Branded Apparel Maker	Detecting insider fraud	• Trusted insider stealing and destroying key data
$100B Diversified Corporation	Predicting risks against your business	• Automating the policy monitoring and evaluation process for configuration change in the infrastructure
Industrial Distributor	Addressing regulatory mandates	• Real-time extensive monitoring of network activity, in addition to PCI mandates

Challenge 1: Protecting Risks against the Business

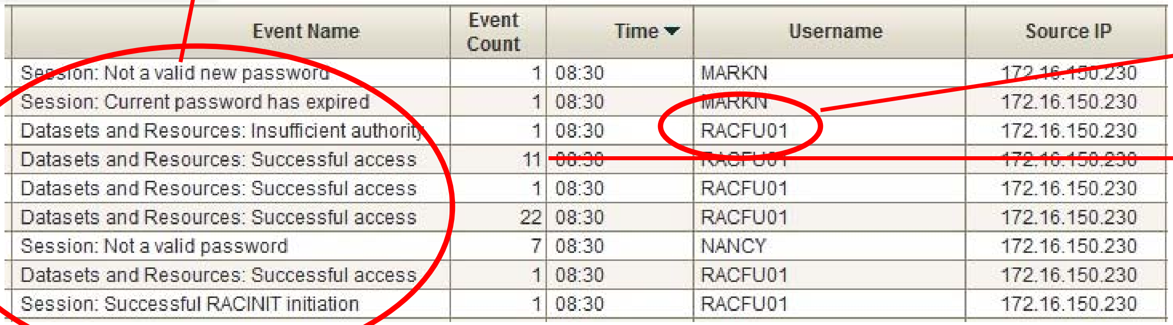
Mainframe Data posted online

Who? What? Where?



	Id		Offense Source	Magnitude	Source IPs
	160	Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events	202.153.48.66		202.153.48.66
	154	Policy: Chat or IM Traffic Detected containing Chat.MSN	10.0.110.17		10.0.110.17
	236	Communication to a know Bot Command and Control containing Chat.IRC	10.0.5.69		10.0.5.69
	148	Sensitive Data in Transit containing Web.Facebook.Application	10.0.240.170		10.0.240.170
	125	Policy: Local: Clear Text Application Usage	10.0.100.104		10.0.100.104
	501	Communication to a known Bot Command and Control containing HTTPWeb	69.20.125.168		69.20.125.168
	150	Login Failures Followed By Success from the same Username	roberta_hite		10.0.5.226
	155	DLP - Potential Data Loss containing Web.MSNLive.Text	10.0.240.251		10.0.240.251
	146	Login Failures Followed By Success to the same Destination IP	80.96.34.22		80.96.34.22

RACF Events



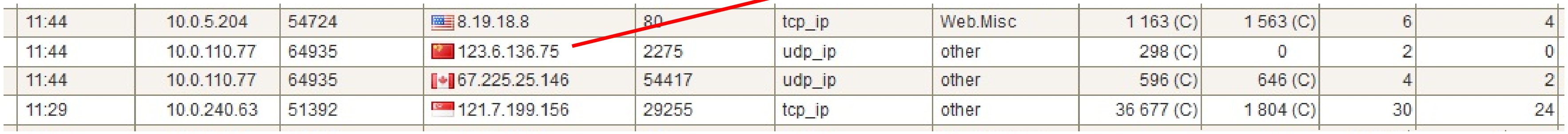
Event Name	Event Count	Time ▾	Username	Source IP
Session: Not a valid new password	1	08:30	MARKN	172.16.150.230
Session: Current password has expired	1	08:30	MARKN	172.16.150.230
Datasets and Resources: Insufficient authority	1	08:30	RACFU01	172.16.150.230
Datasets and Resources: Successful access	11	08:30	RACFU01	172.16.150.230
Datasets and Resources: Successful access	1	08:30	RACFU01	172.16.150.230
Datasets and Resources: Successful access	22	08:30	RACFU01	172.16.150.230
Session: Not a valid password	7	08:30	NANCY	172.16.150.230
Datasets and Resources: Successful access	1	08:30	RACFU01	172.16.150.230
Session: Successful RACINIT initiation	1	08:30	RACFU01	172.16.150.230

Who? RACFU01 user

How many times? 11

Where were they from?

How much data sent?



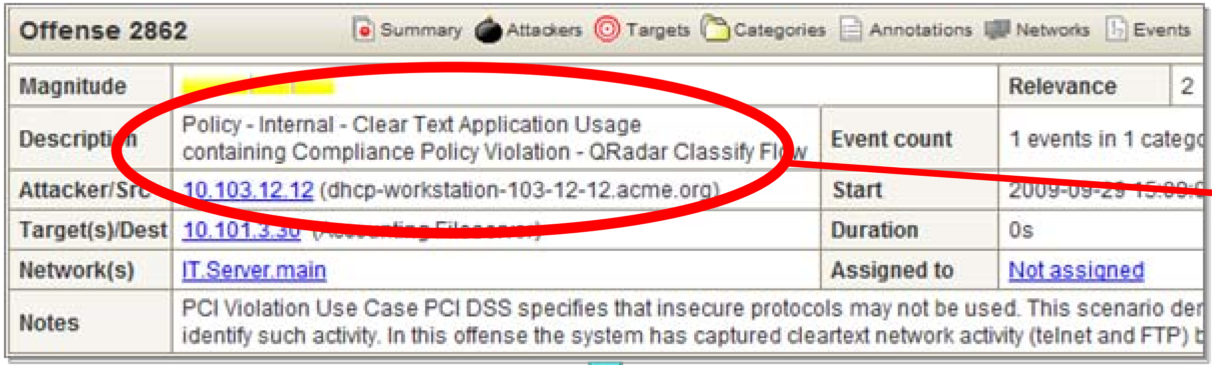
11:44	10.0.5.204	54724	8.19.18.8	80	tcp_ip	Web.Misc	1 163 (C)	1 563 (C)	6	4
11:44	10.0.110.77	64935	123.6.136.75	2275	udp_ip	other	298 (C)	0	2	0
11:44	10.0.110.77	64935	67.225.25.146	54417	udp_ip	other	596 (C)	646 (C)	4	2
11:29	10.0.240.63	51392	121.7.199.156	29255	tcp_ip	other	36 677 (C)	1 804 (C)	30	24

Threat detection in the post-perimeter world

Tracking Mainframe data that is mishandled on other systems

Mainframe, Application and Network level visibility are critical to identify inside threats

Challenge 2: Addressing Regulatory Mandates

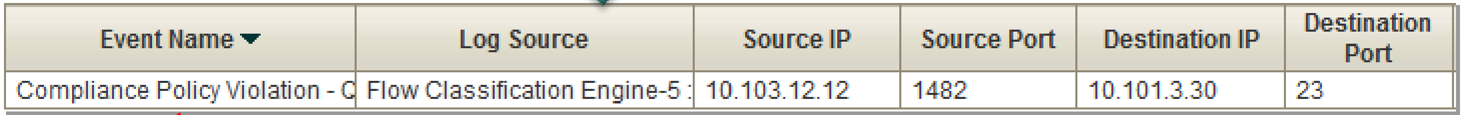


Offense 2862

Magnitude		Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 catego
Attacker/Src	10.103.12.12 (dhcp-workstation-103-12-12.acme.org)	Start	2009-09-29 15:00:0
Target(s)/Dest	10.101.3.30 (Accounting Fileserver)	Duration	0s
Network(s)	IT.Server.main	Assigned to	Not assigned
Notes	PCI Violation Use Case PCI DSS specifies that insecure protocols may not be used. This scenario der identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

Mainframe data PCI compliance at risk?

Real-time detection of possible violation



Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

IBM Security QRadar QFlow saw a cleartext remote access protocol to the mainframe

PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified

Out-of-the-box support for major compliance and regulatory standards

Automated reports, pre-defined correlation rules and dashboards

QRadar benefits in the zOS environment

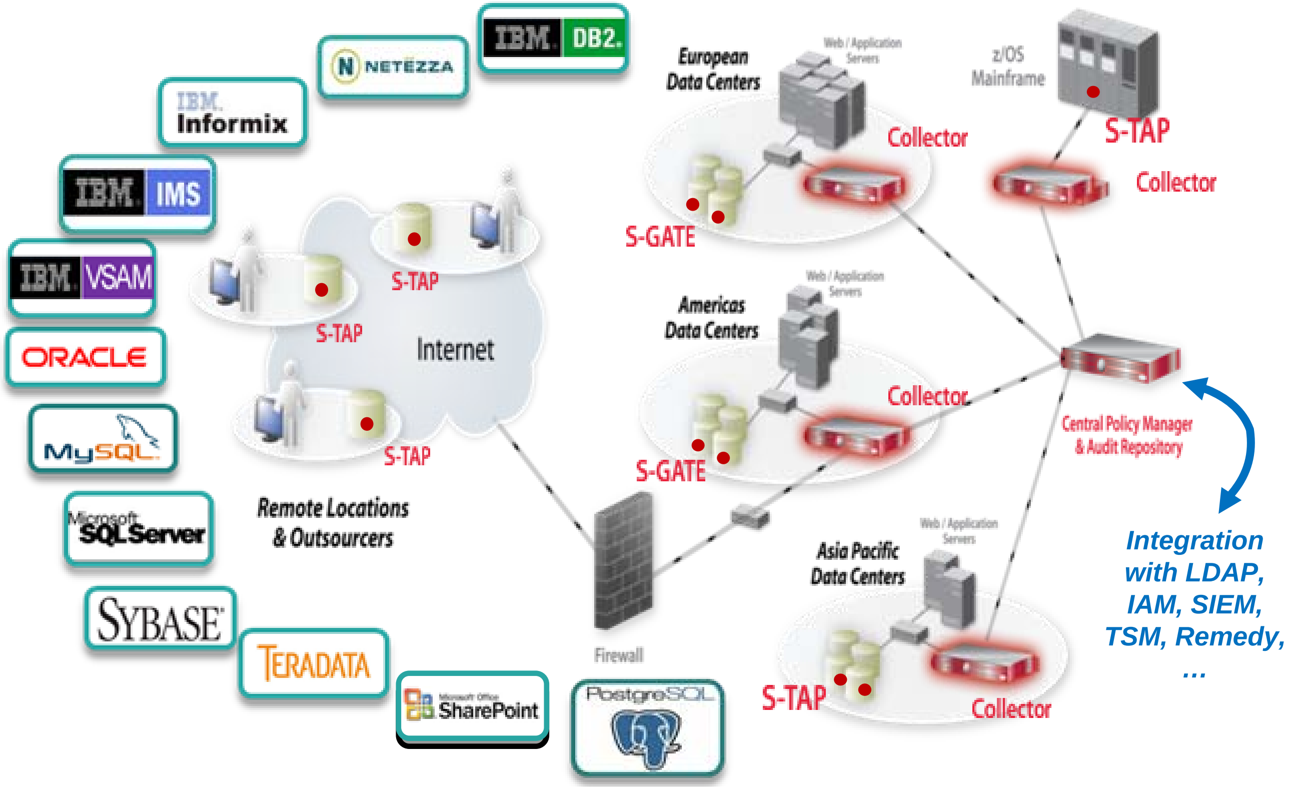
- Consolidates Data Silos by gathering data across mainframes and other systems into one console
- Stores event data in forensically secure database to address regulation mandates
- Complex correlation rules trigger on threats, insider fraud and business risk across the enterprise computing and transmission environment
- Reports on zOS mainframe activity for forensics and regulation mandated auditing

IBM Guardium Provides Real-Time Database Security & Compliance

✓ Continuous, policy-based, real-time monitoring of all database activities, including actions by privileged users

✓ Database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities

✓ Data protection compliance automation

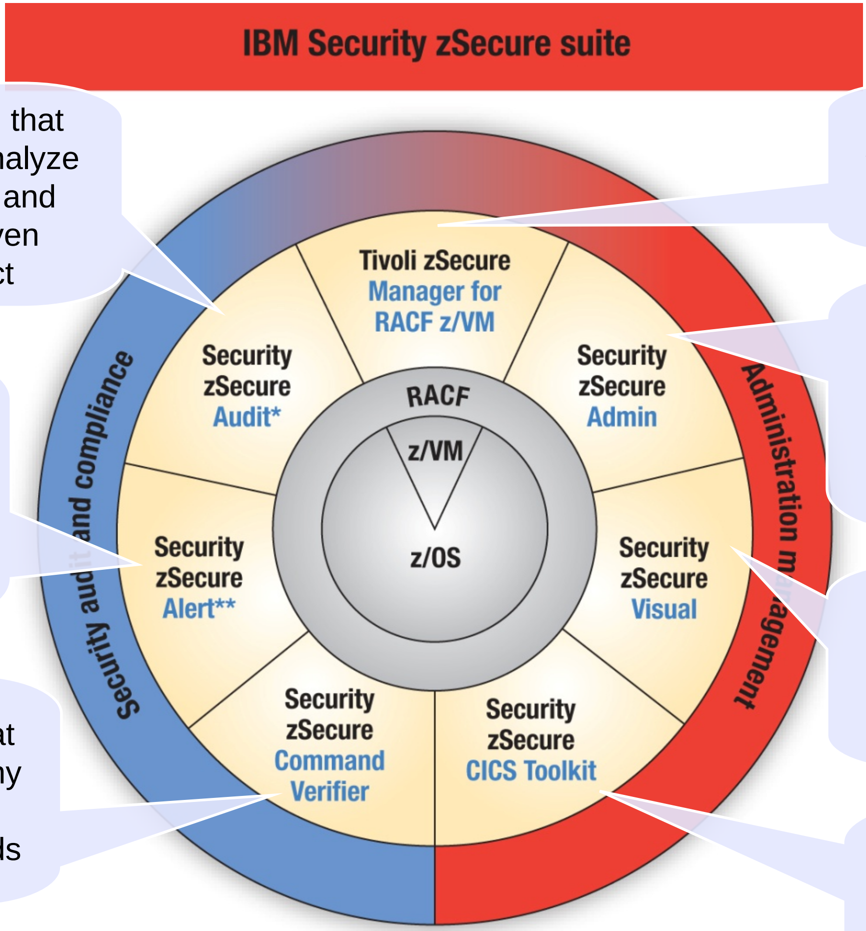


Integration with LDAP, IAM, SIEM, TSM, Remedy, …

Key Characteristics

- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized & suspicious activity
- Granular, real-time policies
  - *Who, what, when, how*
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Introducing the IBM Security zSecure Suite


IBM Security zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures even outside the security product

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

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 plus auditing Linux on System z

Enables more efficient and effective RACF administration and auditing, using significantly less resources. Provides access monitoring, RACF offline, database merge capabilities

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

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources and provides API

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

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

Baseline

- **Why establish a baseline**
  - – Each system will have specific and different characteristics
  - – Know where you started
  - – Know where you are headed
  - – Know where you have gotten

- **Examples**
  - – Freeze an image of your operating system
  - – Unload a copy of your security definitions

Baselines

- **Use the baselines to create “Where we are”**
- **Examples to consider**
  - **z/OS Integrity**
    - **z/OS itself**
    - **System Critical Datasets**
    - **Authorized Libraries**
    - **Program Properties Table (PPT)**
    - **Command Authority (System, Operator)**
    - **User Supervisor Calls (SVCs)**
  - ESM
    - ESM System Options
    - Critical User Attribute (CUA)
    - Public Data Sets and Resources
    - Password (Default and Trivial)
    - ESM Common Problems
- **What do these look like?**

Find mis-configuration and vulnerabilities

- **Situation:**
  - z/OS and RACF protect each other
    - System datasets must be protected…
  - Verifying the protection is time consuming

- **Best Solution Available?:**
  - Individual reports for RACF, PARMLIB, UNIX....
    - Manual correlation and verification?
  - Annual external audit

zSecure Solution

- zSecure Audit takes information from RACF, z/OS, UNIX

  o Identifies inconsistencies and vulnerabilities

  o Shows the privileged users that can chance z/OS, RACF

  - Or bypass security

  o Adhoc reports

  o Automatic reporting and monitoring in batch jobs

AUTOMATION, AUTOMATION, AUTOMATION

Reduce human error and increase security levels

System Critical Datasets

Many system datasets and activities are critical to overall security and effectiveness.

- **SYS1.PARMLIB**
  - The IEASYSxx member of SYS1.PARMLIB contains controlling system parameters that specify how other members are to be used by the system as well as certain operating characteristics.
- **SMF Datasets**
  - Certain system libraries are instrumental to the operation of MVS providing controlling parameters as well as history and audit trail functions. Any violation of those datasets could severely impact system reliability and personnel accountability.
- **Master Catalog**
  - The MVS Master Catalog contains indices used to reference other catalogs and data groups. Write access to the Master Catalog should be restricted. Such access could potentially damage strategic information or, perhaps, render the system unusable.

AND MANY MANY MORE

A Few of the System Critical Datasets – Automatically Checked by IBM Security zSecure

- APF data sets
- LPA data sets
- Page data sets
- Swap data sets
- ESM data sets
- RRSF data sets
- SMF recording data sets
- System dump data set
- TSO user administration data set UADS
- SYS1.NUCLEUS and SYS1.LPALIB
- JES2 and JES3 checkpoint data sets
- JES2 and JES3 spool data sets
- JES2 and JES3 parameter data set
- JES2 and JES3 STC/TSU proclib

- MSTR proclib
- MSTR parameter library
- MSTR VIO administration
- DFHSM data set BCDS, MCDS, OCDS
- HFS data sets
- DMS database DMSFILES
- DMS authorized parameter library
- DMS default parameter library
- CA1 tape management catalog TMC
- DFSMS SCDS and ACDS (integrity)
- IODF file, if DSN could be found
- Couple data sets
- RMM control dataset
- TLMS volume master file VMF
- ABR archive control file ACF

Common ESM Problems

- **USER/GROUP Maintenance**
  - Finding user and grouping inconsistencies
- **PROGRAM Class Maintenance**
  - Check for obsolete conditional permission lists when program definitions have been removed
  - Check for non-existent data set/volume program combinations
  - Checking for program definitions not describing any physical module
- **DATASET Maintenance**
  - Finding and protecting unprotected data sets checks depending on the current protection setting
  - Removing unused discrete definitions - resulting from volume-level operations
  - Finding and removing redundant discrete definitions
  - Removing unused generic definitions (after deletion of 'subject' data sets)
  - Finding and resetting unnecessary ESM-indicated bits (where no discrete definition exists)
- **STARTED Class Maintenance**
  - Finding inconsistencies in started task definitions

Beyond Baseline: Automated Clean up and Control

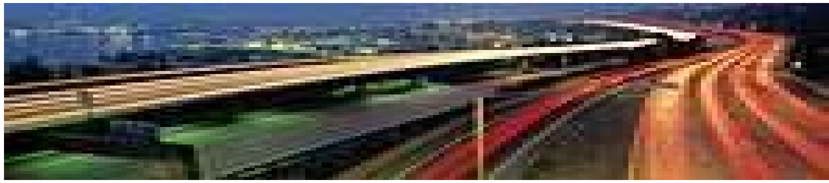
Now you have established the baselines – you can clean up

- **BUT**
  - How do you maintain and prevent re-contamination?
  - After the fact – clean up
    - using SMF event reporting
    - Utilizing your baseline comparison reports
  - Before the fact – prevent the problem
    - Once your policies are defined and codified
    - Establish a means to prevent conditions outside the policies from taking place – control and verify commands, before their execution can undo

AUTOMATE AUTOMATE AUTOMATE

Benefits of Automating with Technology

- Facilitate compliance with security requirements and policies
- Leverage seamless integration with an enterprise-wide view of audit and compliance efforts
- Monitor and audit incidents to help detect and prevent security exposures, as well as assess compliance
- Automate routine administrative tasks to help reduce costs and improve productivity
- Understand the security baseline and when it changes to keep security intelligence at it’s highest and up to date



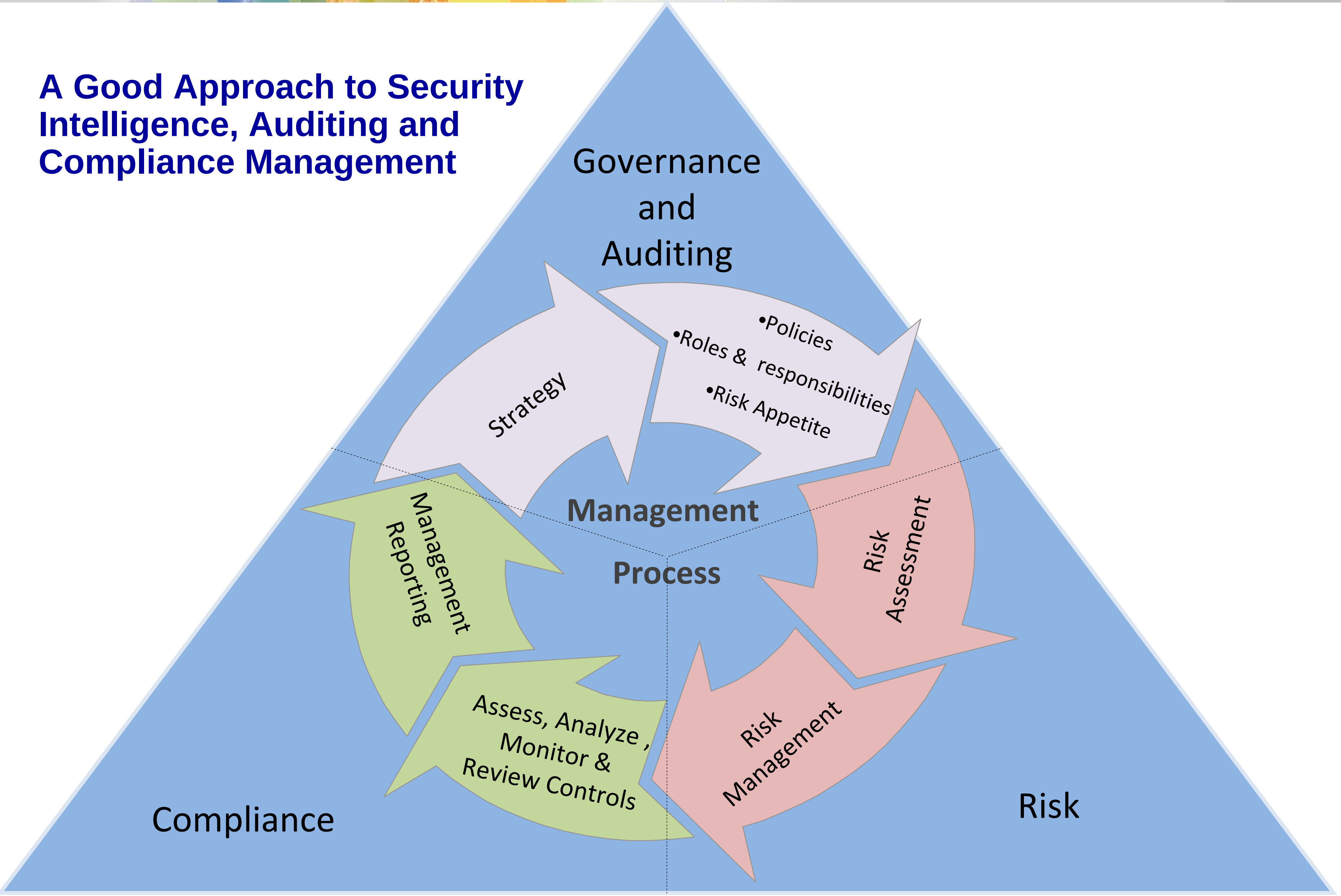
Beyond Baselines – Moving Forward

- **Now**
  - Baselines to measure progress
  - Baselines to compare changes
  - Clean up the environment
  - Prevent subsequent contamination
  - Monitoring the environment

- **You can answer the question:**

How Secure is My Mainframe?

A Good Approach to Security Intelligence, Auditing and Compliance Management



QUESTIONS

?