Security Auditing & Compliance: Best Practices for Today and Beyond

Software Engineering of America

iSecurity

SEA™

About SEA

- Established in 1982
- 9 of the Fortune 10
- 85% of the Fortune 500
- Licenses in over 50 Countries

Agenda

- Starting with Security - Best Practices
- Why Is All This Security Needed Today?
- Auditing & Compliance – Best Practices
- Today's Tools for the Job
- iSecurity
- Security, Auditing & Compliance –Beyond
- Live Demo
- Q&A

Starting with Security – Best Practices

- Written Security Policy
  - Regulators provide an excellent starting point (SOX, PCI, FISMA, HIPAA . . .)
  - PCI contains specific details
  - https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

    (Oct. 2010)
  - COBIT from ISACA to comply with Sarbanes Oxley

Starting with Security – Best Practices

- Rules to Enforce Security Policy
  - Company Policy with teeth
  - Applications designed and written to limit user activity to only authorized activity
- Real-time Alerts of Exceptions to Policy

Starting with Security – Best Practices

- Continuous Monitoring of System Activity
- Continuous Monitoring of Regulators
  - Changes
  - New Versions

Starting with Security – Best Practices

- Types of Policies
  - Physical
    - Protect Your Hardware
    - Locked door to data center, record all entries & exits
    - Fire, water, wind etc damage
  - Software and Data
    - Protect Your System from damage and unauthorized access

Starting with Security – Best Practices

Limit access to *only* authorized users, that they are restricted and monitored to ensure that they are only doing what their job description requires and no more

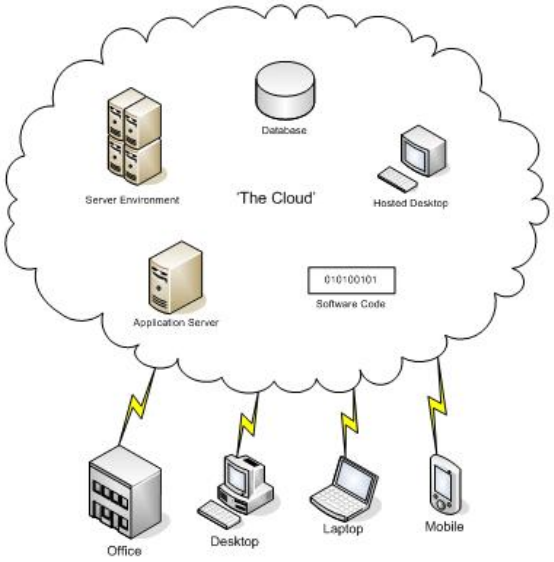
- Just because you work in payroll you should not be browsing the pay records of other people
- Just because you are a big fan of that famous person who was just admitted, you should not be browsing the patient records if you are not on the case

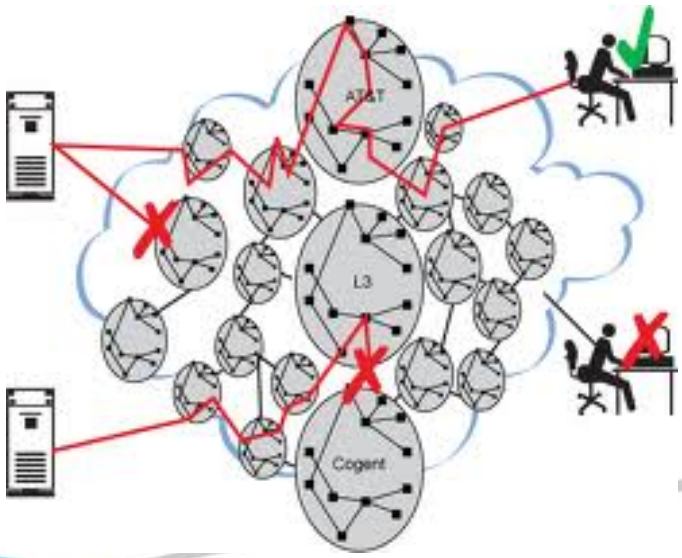
Why Is All This Security Needed Today?

- AS/400 History, Architecture and Security
- IBM Announces System/38
  - Backup and restore
  - Security
  - OS is Object Oriented Architecture (OOA)
  - 64 bit addressing
  - Single level storage
  - No internet
  - IBM PC introduced 8/12/81

Why is All This Security Needed Today?

- AS/400 Architecture today relative to connectivity & security
  - TCP/IP replaces SNA, token ring & Ethernet, replace Twinax
  - Leased lines moving to the CLOUD
- And the information world has changed!



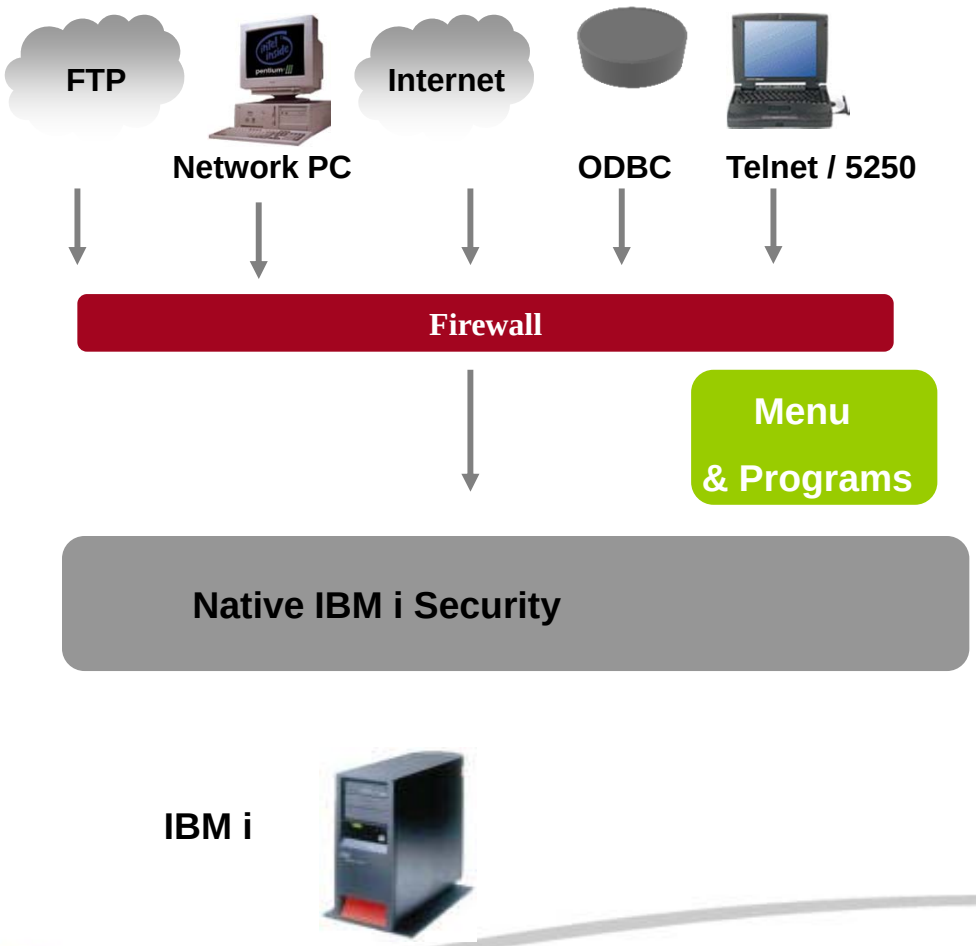


iSecurity

SEA™

IBM i Is Missing A Layer of Security

- Native IBM i security: suitable for stand-alone systems
- External access bypasses IBM security
- The i is vulnerable in network environments
- iSecurity Firewall addresses this.



With Firewall

Why Is All This Security Needed Today?

- Hackers – thieves – governments – invasive internet
  - PC's
  - Cell phones
  - Game boxes
  - Social media
- Today, we have to protect our data, applications, employers, the integrity of the information, ourselves.

Auditing & Compliance

- Regulatory Acts
  - SOX
  - PCI
  - BASEL II
  - FISMA
  - HIPAA
  - ISO
- Audits have become critical

Auditing & Compliance

- Impact of Regulatory Non-Compliance
  - Multi-million Dollar Fines
  - Removal from Service Provider Lists (PCI)
  - All C-level functions (CEO, CIO, CSO, CFO) are personally responsible for security-related issues
  - Reputational Damages
  - No one wants to be on the front page of the NYT for this

Auditing & Compliance **- Best Practices**

- Lessons from the Headlines
  - Use Strong Passwords
  - Rein in Outside Sites
  - Respond Quickly & Proactively

Today's Tools for the Job - Choices

- Write Your Own Apps and Reports
- Download Samples from the Internet and build from there
- Evaluate Vendor Products
- The iSecurity suite of security products are specialized and constantly updated applications with world premier support

iSecurity

- Move to End-to-End Security for your systems.

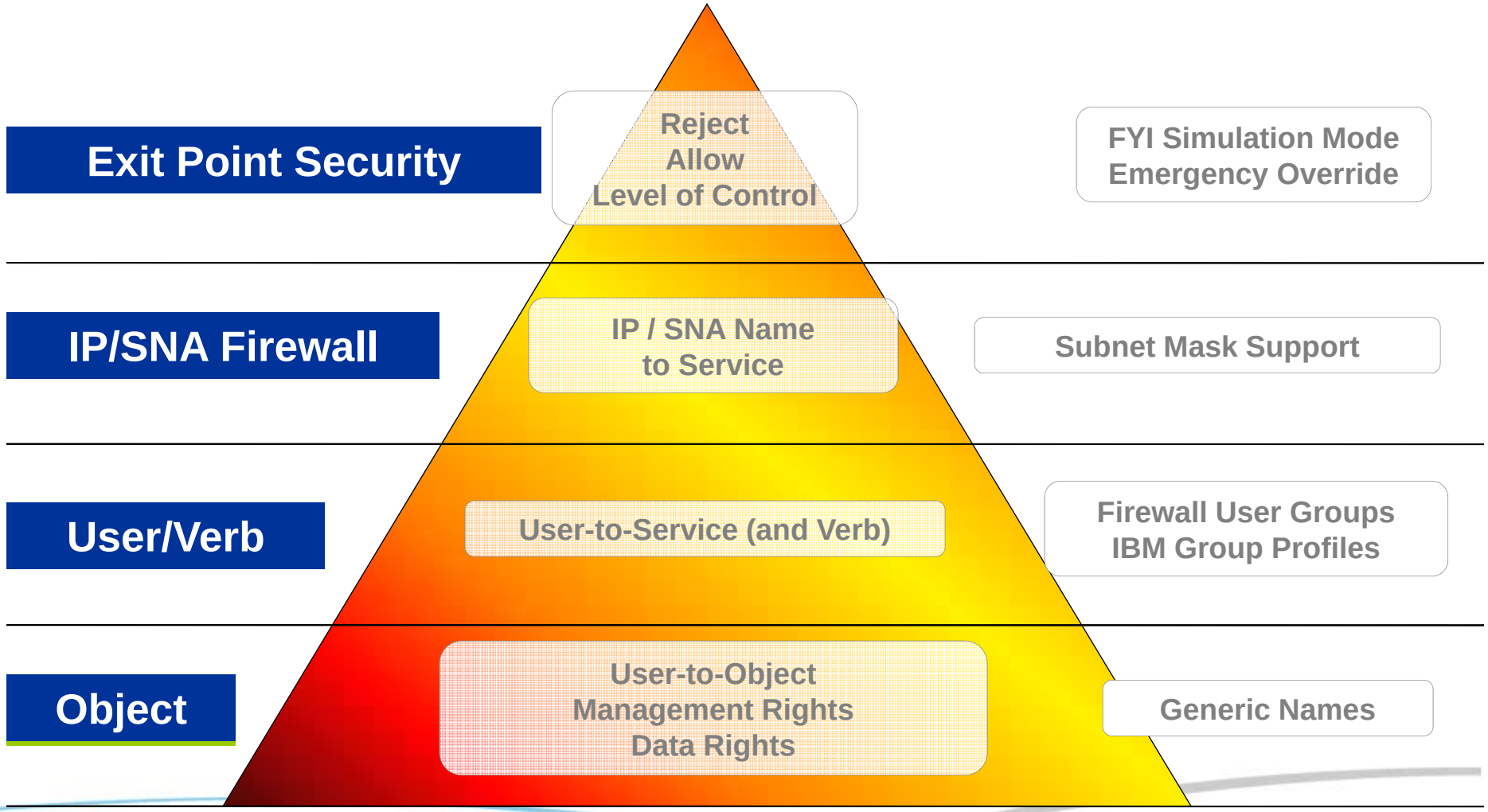
Firewall Gateways

iSecurity Firewall Gateways
- IP Address
- User
- Verb

- Files
- Libraries
- Commands

Other product Gateways
- IP Address

Firewall – Layered Security



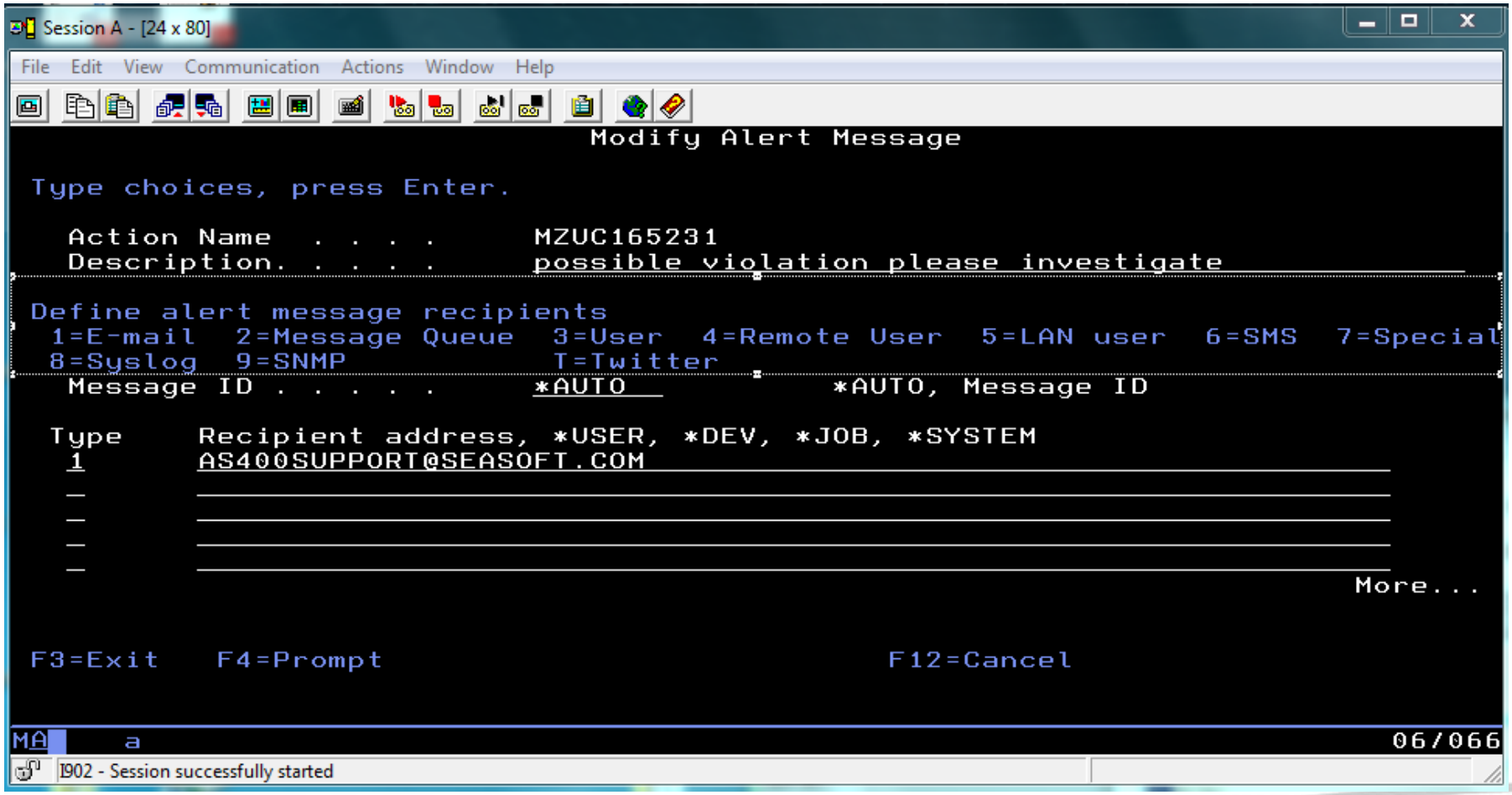
iSecurity

SEA™

Audit

- Local Activity on the i Series
- Real-time monitoring of system related activities
  - » QAUDJRN
- Filtering of events in QAUDJRN
- FULL Alerting, Action & Reporting Capabilities
- Business Intelligence Tool
- Ensure compliance of regulatory acts

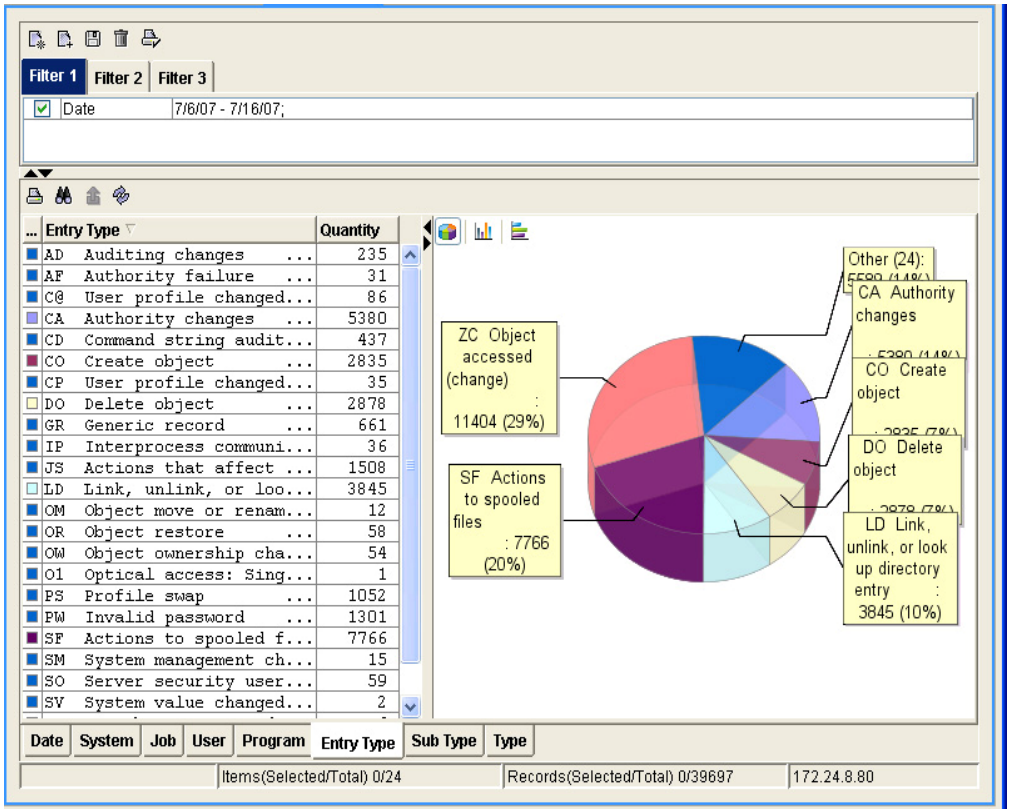
iSecurity Solutions



iSecurity

SEA™

Business Intelligence



GUI Interface

- Graphically analyze Audit / Firewall data
- Display a large quantity of transaction data with minimal storage required.
- Eliminate log scanning
- Print a screen or email it
- Quick and Easy Compliance Monitoring

30

iSecurity

SEA™

Compliance Evaluator

1	2	3	6	7	8	9	14	15	16	21
Sunday, July 05, 2009			Report Filter:		T	Summary				
					(NonBlanks)	Exceptions				

iSecurity Compliance Evaluator

All System Values

System:	S44K1246	S720
Compliance Rating:	58%	64%

Item	Topic	Name	Relative Importance	Current Value	Optimal Value	Rank for Topic	Current Value	Optimal Value	Rank for Topic
All System Values			100%			58%			64%
Previous end of system indicator	*SYSCTL	QABNORMSW		0	0		0	1	
Accounting level	*MSG	QACGLVL		*JOB *PRINT...	*NONE		0	1	
Initial number of active jobs	*ALC	QACTJOB		45			20		
Additional number of active jobs	*ALC	QADLACTJ		30			10		
Spooling ctl block additional storage	*ALC	QADLSPLA		2048			2048		
Additional number of total jobs	*ALC	QADLTOTJ		50			10		
Allow object restore option	*SEC	QALWOBJRS		*ALL	*ALL		*ALL	*ALL	
Allow user domain objects in libraries	*SEC	QALWUSRDM		*ALL	*ALL		*ALL	*ALL	
User assistance level	*SYSCTL	QASTLVL		*ADVANCED	*ADVANCED		*BASIC	*ADVANCED	
Attention program	*SYSCTL	QATNPGM		QCMD QSYS	*ASSIST		QEZMAIN QSYS	*ASSIST	
Auditing control	*SEC	QAUDCTL		*AUDLVL *NOQTEM...	*AUDLVL *OBJAUD...		*AUDLVL *NOQTEM...	*AUDLVL *OBJAUD...	
Auditing end action	*SYSCTL	QAUDENDACN		*NOTIFY	*NOTIFY		*NOTIFY	*NOTIFY	
Force auditing data	*SYSCTL	QAUDFRCLVL		*SYS	*SYS		*SYS	*SYS	
Security auditing level	*SEC	QAUDLVL		*AUTFAIL *CREATE...	*CREATE *DELETE...		*AUTFAIL *CREATE...	*CREATE *DELETE...	
Autoconfigure of remote controllers	*SYSCTL	QAUTORMT		1	1		1	1	
Automatic system disabled reporting	*SYSCTL	QAUTOSPRP		0	0		0	0	
Autoconfigure virtual devices	*SYSCTL	QAUTOVRT		9999	1000-9999		999	1000-9999	
Base storage pool activity level	*STG	QBASACTLVL		35	5-25		25	5-25	
Base storage pool minimum size	*STG	QBASPOOL		256	2000-999999		13107	2000-999999	

Centralized Management

RUNFWQRY QRY(All#REJECTS) SYSTEM (*ALL)

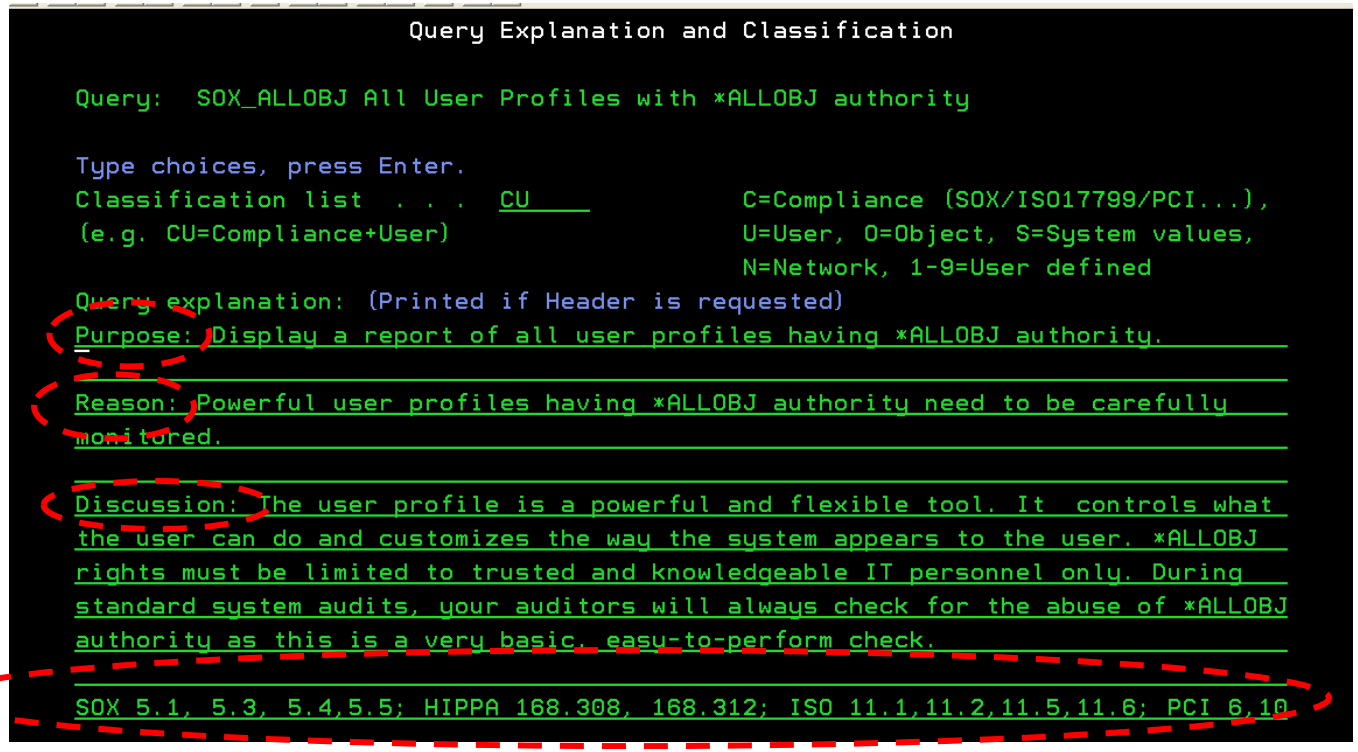
Run Compliance Evaluator report cards over multiple systems

Run queries over multiple systems – SYSLOG, SMTP

Import and export of product configuration

Detailed Compliance Reports

- Compliance Explanations per report
- Specific references to regulatory sections



iSecurity

SEA™

Authority On Demand

- Auditors & Regulators Interest
- Too many people with more access than they require
- Too often give out QSECOFR
- Complete security during a crisis
  - “Break glass” emergency control access

Authority on Demand: Workflow

1. Definition Stage - an authorized System Administrator defines sets of emergency rules

Define Potential Providers
- QSECOFR
- SECADMIN

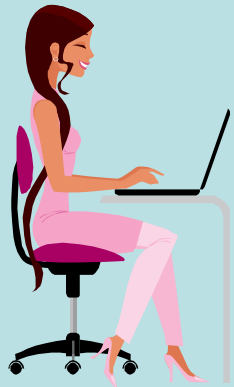
Define Emer. Rules
- "Production"
- "Salary"
- "Weekend"

Rules Details
- ADD/SWAP Auth.
- Rule Description

Notification rules
- E-mail
- SYSLOG
- MSGQ

Rule Conditions
- Date/Time
- Time Group
- IP Address
- Pin Code

2. Emergency Stage - Requester asks for "Production" authority



- Must provide reason
- Enter Pin Code (optional)
- Specify Authority Provider

Get Auth. →

← **Release Auth.**

3. Auditing Stage - by Sysadmin or Auditor

Display/Print AOD & Audit (QAUDJRN) logs by time frame, Provider, or Requester

AP-Journal

- Application level security
- Uses your existing database journal receivers
- Monitor and control by field level & record level
- Query reports, actions and alerts
- A PCI requirement

AP-Journal Business Examples

- **Send** Mail, SMS, SNMP, SYSLOG, Twitter when the INTEREST_RATE changes by more than 0.2%.

- **Who modified** PAYMENTS between 20:00 and 06:00 or during corporate summer vacation?

- **When** did the tariff for overseas transactions change?

- **Which** users, who are not Managers, viewed the confidential PAYMENT_TERMS table since the last business day?

Anti-Virus

- Keeps your IFS from spreading viruses across the network
- Based on CLAM-AV
- Virus signature updates across Internet daily

Security, Auditing & Compliance . . . beyond

- Company Policy
- Outside Auditors
- Outside Regulators
- Legal Responsibilities

iSecurity . . . beyond!

- AP-Journal : Data Area & IFS Support
- Program Change
- Command Tracker
- STRSQL Tracker
  - SQL Interactive/Batch Tracker
- Hierarchical Storage Management (HSM) for iSecurity log files enabling unlimited access to log files
- Segregation of job duties verification

iSecurity Overview

32

iSecurity

SEA™

Support

- Live Support 24x7x365
- Worldwide locations covering multiple time zones
- Training
- Consulting

Live Demo

Q&A
Thank You!

1-516-328-7000
Sales@seasoft.com
http://www.seasoft.com

Outside North America:
marketing@razlee.com
http://www.razlee.com