



security implementation | security consulting | security implementation | security consulting

Leveraging Tivoli zSecure

Beyond just RACF administration

Simon Dodge

New York RACF User Group
TAMPA / S Florida RACF User Group
October 2009

security consulting | security implementation | security consulting | security implementation

This is a User Experience session




- These experiences / opinions are from the presenter
 - Independent of vendor, IBM
- Any errors / inaccuracies are mine, and not IBM
- Always check with current manuals / support teams if in doubt
- Presenter Contact info:
 - sdodge@siconsults.com
 - 404 327 8781

security consulting and implementation

Basic Administration & Auditing tasks SiCon
inc

(we expect this functionality)


- zSecure Admin
 - Administration tool: Display / Modify RACF profiles
 - RACF Reporting
- zSecure Audit
 - zOS + RACF auditing
 - SMF reporting
- zSecure CICS toolkit
 - RACF admin via CICS programs, screens



security consulting and implementation

Above & Beyond Administration SiCon
inc

- zSecure Admin/zAudit
 - RACF Reporting: Comparing RACF to Environment
 - RACF Reporting: Merging data together
 - RACF Offline: Ability to manage an alternate RACF db
 - Powerful programming/query language, CARLA
- zSecure Command Verifier (previously known as zLock)
 - Enforcing your policies on RACF administrators
 - Audit trail of RACF commands



security consulting and implementation

Agenda..

SiCon
inc

Examples of VERIFY functions

security consulting and implementation

VERIFY functions
4 examples of the 15 functions are

SiCon
inc

- **VERIFY PROGRAM**
 - Does ADDMEM on a PROGRAM profile actually exist ?
- **VERIFY PGMEXIST**
 - Does program actually reside in that library ?
- **VERIFY STC**
 - Are SPT(ICHRIN03), STARTED, STC proclibs "in sync" ?
- **VERIFY SENSITIVE**
 - Are sensitive zOS datasets adequately protected ?

security consulting and implementation

VERIFY PROGRAM

SiCon
inc

- Verifies that ADDMEM dsname actually exists
- Builds possible RACF commands to rectify

```
/* Commands generated by VERIFY PROGRAM */  
  
ralter program **      delmem('SHARE.IMS.LOADLIB')  
  
ralter program TSBXMDR delmem('SHARE.IMS.TEST.LOADLIB')  
ralter program TSBXMDR delmem('SHARE.ZOS.ALS.LOADLIB')  
  
ralter program FDR*   delmem('SHARE.ZOS.LOADLIB')  
  
ralter program **      delmem('SHARE.ZOS.ZAUDIT.V190.SCKRLOAD')  
ralter program CKR*   delmem('SHARE.ZOS.ZAUDIT.V190.SCKRLOAD')  
  
SETROPTS REFRESH WHEN(PROGRAM)
```

security consulting and implementation

VERIFY PGMEXIST

SiCon
inc

- Verifies that PROGRAM actually exists as load module in library

```
/* Commands generated by VERIFY PGMEXIST */  
  
rdelete program WIZARD  
  
SETROPTS REFRESH WHEN(PROGRAM)
```

security consulting and implementation

REPORT STC

SiCon
inc

- Shows data from STARTED (& ICHRIN03), JES STC proclibs

```
STARTED TASK OVERVIEW 27 Jan 2009 16:10
```

Procname	Userid	Flags	Group	Sys	SubshLib	Last updt	By	STARTED profile	U	Volume	Dataset	
APPC	STCAPPC	DS	STC	ATL1	JES2h	9	MSTR	APPC.**	N	COUS2P	SYS1.IBM.PROCLIB	
CICSP382	STCCICS	DS	STC	ATL4	JES2h	6	3Sep08	SYSPROG	CICSP**	N	COLA10	CICS.STC.EMER.PROCLIB
CICSP382	STCCICS	DS	STC	ATL4	JES2h	6	10Aug08	SYSPROG	CICSP**	N	COLA10	CICS.STC.PROD.PROCLIB
CICSP389	STCCICS	DS	STC	ATL4	JES2	6	10Aug08	SYSPROG	CICSP**	N	COLA10	CICS.STC.PROD.PROCLIB
BPXAS	STCKERN	DS	STC	ATL1	JES2	9	MSTR	BPXAS.**	N	COUS2P	SYS1.IBM.PROCLIB	
BPXOINIT	STCKERN	DS	STC	ATL1	JES2	9	MSTR	BPXOINIT.**	N	COUS2P	SYS1.IBM.PROCLIB	
OMVS	STCKERN	DS	STC	ATL1	JES2	9	MSTR	OMVS.**	N	COUS2P	SYS1.IBM.PROCLIB	

security consulting and implementation

VERIFY STC

SiCon
inc

- Verifies that ADDMEM dsname actually exists
- Builds possible RACF commands to rectify

```
/* Commands generated by VERIFY STC */  
  
rdelete started ABNDTEST.**  
  
rdelete started C2POLICE.**  
  
rdelete started C2PACMON.**  
  
SETROPTS REFRESH RACLIST(STARTED) /* POSIT 66 */
```

security consulting and implementation

REPORT SENSITIVE

SiCon
inc

- Shows how sensitive system datasets are protected and identifies any shortcomings according to selected policy
 - C1, C2, B1, or zSecure (default) which is a hybrid suitable for most commercial institutions

```
S E N S I T I V E   D A T A S E T   P R O T E C T I O N   O V E R V I E W           28 Jan 2009   page   1
```

Type	Sensitivity	Volume	Datasetname	User/group	access	program	UACC	S/F	Erase	Shortcomings
GENERIC			CICS.*.SDF%AUTH.APF	\$CICS	OWNER		NONE	R	No	Update fail audit
nvsam	APF	library	CIC014 CICS.TS310.SDFHAUTH.APF	STCICIS	READ					
nvsam	APF	library	CIC014 CICS.TS310.SDFJAUTH.APF	BATCH	READ					
nvsam	APF	library	CIC025 CICS.TS320.SDFHAUTH.APF	CICS	ALTER					
nvsam	APF	library	CIC025 CICS.TS320.SDFJAUTH.APF							
GENERIC			RACF.**	\$RACF	OWNER		NONE	R	R	Yes
nvsam	RACF	prim	RACK01 RACF.PRIMARY	SECADMIN	READ	CKRCARLA				
nvsam	RACF	back	RACK05 RACF.BACKUP	AUDIT	READ	CKRCARLA				
				SECBATCH	READ	CKRCARLA				
				SYSPROG	ALTER					

security consulting and implementation

VERIFY SENSITIVE

SiCon
inc

- Builds commands to address shortcomings

```
/* Commands generated by VERIFY SENSITIVE */  
altdsd 'CICS.*.SDF%AUTH.APF' audit(success(update),failure(read))  
SETROPTS REFRESH GENERIC(DATASET)
```


security consulting and implementation

Types of datasets automatically located via REPORT / VERIFY SENSITIVE

SiCon
inc

Sensitivity	Sensitivity	Sensitivity
APF lib+Lnk	ICSF CKDS	RACF back
APF library	ICSF PKDS	RACF prim
Catalog	IPL Nucleus	RRSFdataset
Couple Alt	JES2 Ckpt	System REXX
Couple Prim	JES2 Spool	SMF dataset
CA1 TMC	LPA list	SMS ACDS
DmsFiles	MSTR prmlib	SMS COMMDS
HFS dataset	MSTR STClib	SMS SCDS
HSM BCDS	NoAPFnonSMS	STC proclib
HSM MCDS	NoAPFnoCtlg	TSU proclib
HSM OCDS	Pagedataset	

This is just a list of what was observed on my test system. See manual for full list (zSecure Audit will run on ACF2, TSS)




security consulting and implementation

Agenda..


SiCon
inc

RACF - Offline



security consulting and implementation


RACF Offline



- Component of zSecure Admin
 - Previously available from BCSC
 - IBM acquired after the Consul acquisition

- Allows you to manage an “Offline” RACF database
 - IE not current live/backup database
 - Prepare “What If” scenarios and report
 - Build “Massive changes” and report
 - SMF reporting can distinguish between real RACF updates and Offline RACF updates

- Can avoid the need for a separate testing lpar just for a test RACF database



security consulting and implementation

Agenda..



CARLA language



security consulting and implementation

CARLa programming language

SiCon
inc

Previously known as Consul Auditing and Reporting
Language

Now recursively known as CARLA Auditing and Reporting
Language

- Query type language
 - -vs- traditional Open/Close/Read/Write/If/Then/Else
- Multiple data types (50+)
- including RACF, SMF
- Output via SYSOUT, DSN, SMTP (eMail), XML



security consulting and implementation

ISPF interface of zSecure

SiCon
inc

The ISPF panels build CARLA queries


This means you can easily copy and modify a panel query
so that results look just as you want

- Move fields around
- Add/Delete fields
- No need to build “homegrown” ISPF dialog manager aps
- Very easy to build custom displays




security consulting and implementation

Agenda..



SiCon
inc

Examples of custom CARLA coding



security consulting and implementation

Custom ISPF panel


SiCon
inc


These 6 lines of CARLA code:

```
newlist type=racf st='Profiles in NODES class'  
select class=NODES  
display searchkey(key,nondisp1) key(key,26),  
       uacc owner memcnt(1,'#'),  
       memlst('Member',8,firstonly),  
       create(9) instdata
```

Produce this display panel

```
IBM Tivoli zSecure RACF display                               Line 1 of 26  
Command ==>                                                Scroll==> PAGE  
Profiles in NODES class                                     28 Jan 2009 10:59
```

Profile key	UACC	Owner	#	Member	CreateDat	InstData
___ CITINJE.USER%.*	CONTROL	\$JES	1	&SUSER	04Apr2008	NJE: HORUS
___ DOGS.USER%.*	CONTROL	\$JES	1	NJE001	21May2004	NJE: ZUES
___ FED.USER%.*	CONTROL	\$JES	1	NJE002	14Apr2004	NJE: BODACIA
___ OFFSHORE.USER%.*	CONTROL	\$JES	1	&SUSER	04Apr2008	NJE: PATRICK



security consulting and implementation

Custom Group Report page 1 of 2 SiCon
inc

Group analysis showing their usage for ATL 26Jan2009 19:00
Possible cleanup if NO Userids + NO SubGrps + NO DsnProf + NO Permits + NO Owing

Group Structure	U	Userids	SubGrps	DsnProf	Permits	Owing	OmvgsGID
SYS1		12	6	13	23	56	
OMVS			6			6	
APPL			3		36	3	
DEPT28		11					1000
DEPT73							1001
@AUDIT					2018		
PACMAN					1		
DEPT08		3				1	
DEPT05		2286				2228	1000
PSWD		21			158		
SEQ		25		19	553	3	
BANK01		2			15	2	
IS		2		1981			
WAS				1288			
WILLBE				1			
PQR			3	59		3	
STU				7	184		
JKL			2	61	2	2	

security consulting and implementation

Custom Group Report page 2 of 2 SiCon
inc

Group analysis showing their usage for ATL 26Jan2009 19:00
Possible cleanup if NO Userids + NO SubGrps + NO DsnProf + NO Permits + NO Owing

Group Structure	U	Userids	SubGrps	DsnProf	Permits	Owing	OmvgsGID
BAT		4	1	15		1	
MAN		70	2	6	2366	2	
CICS			1	1	4	1	
IMS		12		10	921		
DB2			57			57	
DEV		275		24	1402		
MEMOREX		72	48			48	
DEPT24		683	28			707	1000
DEPT17		58			1	61	1001
@ROLENEW		3302			900		
HAYSTACK		45	17		47	17	
DEPT80		51	7		18	60	10004
MERGER	U					2	
@ROLEOC4	U	403					
@ROLE913	U	17000			1083		
\$LOB01	U	32702	2			32253	
\$LOB02	U	6892	1			6848	1006

security consulting and implementation

Groups with duplicated access Custom report

SiCon
inc

- Too many groups that had identical access; Wanted to identify them and combine/consolidate them

Groups that have identical RACF access and Owner 6 Jan 2009 11:28

Grps	Group	U	Users	Owner	Resources (Access/Class/Profile)
26	GROUPRCE	567	SIMON		R MDSNSP SHAR.*.ICM*.EXECUTE
	GROUPERE	109	SIMON		R MDSNSP SHAR.*.ICM*.EXECUTE
	GROUPGPS	33	SIMON		R MDSNSP SHAR.*.ICM*.EXECUTE
	GROUPPSS	5	SIMON		R MDSNSP SHAR.*.ICM*.EXECUTE
	GROUPBNE	4	SIMON		R MDSNSP SHAR.*.ICM*.EXECUTE
	...				
11	GRP1455	70	FRANK		R EJBROLE SHR2.AddCustomer R EJBROLE SHR2.GetCustomerDetails R EJBROLE SHR2.IDandVerifyByAccount R GIMS CUSTINQ R GIMS BALINQ U MQQUEUE MQ*.XX.YYY.ACCT

security consulting and implementation

Reporting from multiple RACF databases

SiCon
inc

Activity report 22 Jan 2009 07:47
Last Connect dates

Userid	Site	LastConn
ACMEB01P	ATLANTA	22Jan2009
	LONDON	13Jan2008
	MUNICH	13Jan2008
ACMEC02P	LONDON	21Jan2009
	MUNICH	07Dec2008
ACMEH01T	NEWYORK	12Sep2007


Simple
CARLA
coding

Userid	Atlanta	London	Munich	NewYork
ACMEB01P	22Jan2009	13Jan2008	13Jan2008	
ACMEC02P		21Jan2009	07Dec2009	
ACMEH01T				12Sep2007

Exploits
Deftype
lookups
(needs
extra
step)

security consulting and implementation

Custom report Differences in RRSF synced databases



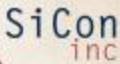
ACME CONFIDENTIAL 22 Jan 2009 07:52 page 1
Weekly RACF Database compare has finished

Site	Timestamp	Users	Grps	Dataset	General	Connect	Permits	Cond	Mbrs
ATL	22Jan2009 07:47	116192	18632	16183	69740	753667	1885301	141	41593
ORL	22Jan2009 07:47	116192	18632	16183	69740	753667	1885301	141	41593
NYC	22Jan2009 07:45	116192	18632	16183	69740	753667	1885299	141	41593

OK: RPT01 Installation data is consistent
OK: RPT10 Userids are consistent
OK: RPT11 Userid segments are consistent
OK: RPT12 OMVS UIDs are consistent
OK: RPT14 CLAUTH lists are consistent
OK: RPT15 OMVS UIDs are unique (No UID is shared)
OK: RPT20 Groups are consistent
OK: RPT21 Group segments are consistent
OK: RPT22 OMVS GIDs are consistent
OK: RPT24 SubGroups are consistent
OK: RPT25 OMVS GIDs are unique (No GID is shared)
OK: RPT30 Connects are consistent
OK: RPT31 Connect Authorities are consistent
OK: RPT40 Dataset profiles are consistent
OK: RPT41 Dataset segments are consistent
=> RPT42 Access list comparison found differences in DATASET
OK: RPT50 Resource profiles are consistent
OK: RPT51 General segments are consistent
=> RPT52 Access list comparison found differences in GIMS
OK: RPT53 APPLDATA is consistent
OK: RPT54 Member lists are consistent
OK: RPT55 STDATA is consistent
OK: RPT56 Conditional Access lists are consistent
OK: RPT57 CDTINFO is consistent
OK: RPT61 UserData is consistent

security consulting and implementation


Custom report Dataset profiles with no datasets/usage



Profile name **SYS1.SHARE.****


UsrNm Flg UsrData

NODSN**ATL** 40 21Oct2007 Was audit(failures(READ))
NODSN**NYC** 40 21Oct2007 Was audit(failures(READ))
NODSN**LON** 40 21Oct2007 Was audit(failures(READ))
EMPTYDLY 40 21Jan2009 Last SMF monitoring




security consulting and implementation

Custom report HLQ analysis




- Common administrative issue concerns catalog aliases
- Not always clear who should be defining/deleting them
 - Or better said, who cleans them up
- Frequently see:
 - Aliases for HLQ's that don't exist in RACF
 - Missing Aliases
 - Missing Dataset profiles
 - Various other inconsistencies



security consulting and implementation


Custom HLQ Analysis Sample summary report



page 1 of 2

RACF / Catalog Alias / VTOC / HSM MCD / TMC analysis 26 Jan 2009 16:03
See detailed reports for each combination

-- RACF --						
HLQ	Dataset	Alias	MCD	Many	in	Concerns
			TMC			
Userid	Profs	Alias	Dsns	317	Rpt1	OK/normal: Userid with protected data
Userid	Profs	Alias	NoDsns	601	Rpt2	No datasets
Userid	Profs	NoAlias	Dsns	0		
Userid	Profs	NoAlias	NoDsns	80	Rpt4	Why have dataset profile?
Userid	NoProf	Alias	Dsns	6	Rpt5	Missing profile
Userid	NoProf	Alias	NoDsns	504	Rpt6	Missing profile, No datasets
Userid	NoProf	NoAlias	Dsns	5	Rpt7	Missing profile, Missing Alias
Userid	NoProf	NoAlias	NoDsns	124984	Rpt8	OK/normal: End user with no datasets
TSOusr	Profs	Alias	Dsns	2302	Rpt9	OK/Normal: TSO user with protected da
TSOusr	Profs	Alias	NoDsns	571	Rpt10	Why set up as TSO user?
TSOusr	Profs	NoAlias	Dsns	0		
TSOusr	Profs	NoAlias	NoDsns	15	Rpt12	Why set up as TSO user?
TSOusr	NoProf	Alias	Dsns	35	Rpt13	Missing profile
TSOusr	NoProf	Alias	NoDsns	8	Rpt14	Missing profile
TSOusr	NoProf	NoAlias	Dsns	0		
TSOusr	NoProf	NoAlias	NoDsns	11	Rpt16	Why setup as TSO user ?



security consulting and implementation

Custom HLQ Analysis Sample summary report

page 2 of 2

SiCon
inc

RACF / Catalog Alias / VTOC / HSM MCD / TMC analysis 26 Jan 2009 16:03
See detailed reports for each combination

-- RACF	-- Catalog	VTOC	How	Details	Concerns	
Hlq	Dataset	Alias	MCD	Many	in	
			TMC			
Group	Profs	Alias	Dsns	727	Rpt17	OK/normal: Group with protected dsns
Group	Profs	Alias	NoDsns	542	Rpt18	No datasets
Group	Profs	NoAlias	Dsns	11	Rpt19	Missing Alias
Group	Profs	NoAlias	NoDsns	192	Rpt20	Why have dataset profile?
Group	NoProf	Alias	Dsns	4	Rpt21	Missing profile
Group	NoProf	Alias	NoDsns	25	Rpt22	Why have alias ?
Group	NoProf	NoAlias	Dsns	0		
Group	NoProf	NoAlias	NoDsns	16941	Rpt24	OK/normal: Group with no dsns
No RACF		Alias	Dsns	100	Rpt25	HLQ not in RACF
No RACF		Alias	NoDsns	1918	Rpt26	HLQ not in RACF, No datasets
No RACF		NoAlias	Dsns	111	Rpt27	HLQ not in RACF, Missing alias

security consulting and implementation

Custom Data extracts for compliance feeds

SiCon
inc

Can easily write data in CSV format

No white space

Recent implementation reduced space of data by 88%

```
CICSDFLTUSER, PLEX2, CICSUNKN, 33 regions, Yes, Yes
MUSASSPROPCNTL, PLEX2, CICS.**, STCCICS, Found
CLASSREQACTIVE, PLEX1, $POLICY, Yes
PROFREQMQ, PLEX3, MQADMIN, *.NO.PROCESS.CHECKS, Missing,,,
RACFGLOBAL, PLEX4, GLOBAL, DATASET, SYS1.*.CATALOG/UPDATE, MatchFound
RACFSHAREUID, ACME, UID 1234 shared by 2 users,,
SENSDSNAUD, PLEX2, GENERIC, RACF.PRIMARY.**, RACF.PRIMARY, READ, R
STCTRUSTED, PLEX1, JES2, **, STCJES, STC
USERMULTUID, ACME, SDODGE has 2 UIDs,,
```

security consulting and implementation

Custom use of "UserData" Approvals for "Public" access

SiCon
inc

```

Profile name      SYS1.SHARE.**

User      Access  ACL id  When          Name          InstData
- any -    READ    *
-group-   ALTER    GODS          CHANGE BOY
BATCHXY   ALTER    BATCHXY       XY PROD CA7  BATCH ID

Safeguards
Erase on scratch          No
Audit access success/failures R

Other permissions
Allow all accesses        WARNING No
Universal access authority NONE

Mandatory Access Control
Security label
Security level

Statistics
Creating user's connect group TECH
Creation date                26Oct97

UsrNm      UserData
PublicOK   READ      25Sep2008 REQ: 759e9f58a8b701000000C09D000003
    
```

security consulting and implementation

Custom use of "UserData" Tracking TSO logons

SiCon
inc

```

zSecure Audit for RACF Display Selection
Command ==>>>                               Line 1 of 4
                                                Scroll==>> PAGE

  Name      Summary Title
  ---      -
  TSOALL    2955 All Folks with a TSO segment
  TSOUSED   2103 All Folks who have logged on to TSO
  TSOWHY    861 Folks with a TSO segment who have -not- used it
  TSOgone   9 Folks who no longer have a TSO segment but have used it

Userid  Name      ProcName LastUsed
SDODGE  DODGE, SIMON  IKJACCNT 20Jan2009

TSO Logon was observed:

Where xx      When
USETSONY 20Jan2009
USETSOGA 23Jan2009
USETSOUK 26Jan2009
    
```

security consulting and implementation

SiCon
inc

Agenda..

Command Verifier

Brief overview,

Six examples of administrative controls..




security consulting and implementation

SiCon
inc

Command Verifier (pka zLock, CVO)

- Intercepts RACF commands allowing to you implement additional layer of controls on top of normal RACF rules.
 - Using RACF profiles to control who can perform functions
 - Such as using certain keywords or values
 - System SPECIAL no longer SuperGod
- Can also track command activity, things like:
 - When was that permit issued/deleted ?
 - When was that profile put in WARNING ?
 - When was that segment added/deleted ?
 - When did “so and so” get OPERATIONS ?
 - WHO did that ?



security consulting and implementation

CV Example 1

SiCon
inc

- Giving out SPECIAL / OPERATIONS / AUDITOR
- C4R.USER.ATTR.SPECIAL.<owner>.<userid>
- C4R.USER.ATTR.OPERATIONS.<owner>.<userid>
- C4R.USER.ATTR.AUDITOR.<owner>.<userid>
- Eg: C4R.USER.ATTR.SPECIAL.**

```
alu ANUBIS special  
C4R480E Special attribute not allowed, command  
terminated
```

security consulting and implementation

CV Example 2

SiCon
inc

- Customer needed to control all aspects of management of production datasets; All Prod HLQs were Pxxx
- Profile **creation** controlled via:
 - C4R.DATASET.ID.P%%.**
- Profile **UACC** controlled via:
 - C4R.DATASET.UACC.P%%.**
- **Permits** controlled via:
 - C4R.DATASET.ACL.*.*.P%%.**
- **Warning** controlled via:
 - C4R.DATASET.ATTR.WARNING.P%%.**

security consulting and implementation

CV Example 3

SiCon
inc

- Customer wanted to prevent Group STCCA7 being used in a PERMIT command
- For PERMIT to work you must have UPDATE access to:
 - C4R.<class>.ACL.<id>.<access>.<profile>
- Specification of ID(STCCA7) is therefore controlled via:
 - C4R.*.ACL.STCCA7.**

```
permit 'THOR.**' id(stcca7) access(read)
```

```
C4R601E ACL setting STCCA7 READ not allowed, command terminated
```

security consulting and implementation

CV Example 4

SiCon
inc

- Activated EGN 4 years ago; Many folks still create new dataset profiles *hlq.**.** L
- Wanted to control creation of trailing *.*.***
 - C4R.DATASET.ID.**.+.

```
ADDSD 'ISIS.TMP.**.*'
```


```
C4R640E Define/Delete DATASET ISIS.TMP.**.* not allowed, command terminated
```

security consulting and implementation

CV Example 5

SiCon inc

- Inserting a *default* value different from RACF default
 - Useful when RACF default is not appropriate
 - Especially if you want different defaults for different profiles
- `C4R.MDSN*./OWNER.** APPLDATA('$DB2')`
 - / è Default specification
- Now if you issue `RDEF MDSNxx xxxx` and omit `OWNER`, it will be inserted for you: `OWNER($DB2)`




security consulting and implementation

CV Example 6

SiCon inc

- Forcing a *mandatory* value
- `C4R.GCICSTRN.=OWNER.** APPLDATA('$CICS')`
 - = è Mandatory specification
- Now if you issue `RDEF GCICSTRN xxx` and omit `OWNER`, it will be inserted for you: `OWNER($CICS)`
- Now if you specify an `OWNER` other than `$CICS`, it will be
 - changed to `$CICS`, if you have `UPDATE`, or
 - Rejected if `< UPDATE`





security consulting and implementation

Agenda..

Command Verifier

Audit Trail overview,



Two examples of Command Audit Trail..



security consulting and implementation


Command Verifier Audit Trail

- Optional audit trail maintained in affected RACF profiles
- Support five types of activities
 - Segment changes
 - Attribute changes
 - Group Connect changes
 - Access list changes
 - Member list changes
- Can control WHO can see this output
 - Is added on to end of LISTxxx command




security consulting and implementation

Audit trail Example 1: LISTUSER



```
USER=ANUBIS  NAME=GUESS WHO      OWNER=SECADMIN  CREATED=03.232
... Lines snipped ...
SECURITY-LABEL=NONE SPECIFIED
C4R736I Command Audit Trail for USER ANUBIS
C4R739I Segment:  CICS      Added on 06.087/16:28 by SEKHMET
C4R739I             OMVS      Added on 08.053/10:10 by ODIN
C4R739I             WORK      Added on 06.087/16:29 by SEKHMET
C4R739I  Attrib:  UAUDIT    Removed on 07.332/15:06 by SEKHMET
C4R739I             Added on 07.332/15:21 by GEB
C4R739I             AUDITOR  Removed on 07.303/10:33 by SEKHMET
C4R739I             Added on 07.313/11:37 by GEB
C4R739I             OWNER    Changed on 08.108/09:16 by OSIRIS
C4R739I             DFLTGRP  Changed on 08.108/09:16 by OSIRIS
C4R739I             NAME     Changed on 08.120/11:19 by NUT
C4R739I  Connect:  RC1772  Removed on 07.190/12:39 by PROMETHU
C4R739I             SYS1     Removed on 07.213/12:43 by NUT
C4R739I             @SECLSE  Added on 07.298/12:34 by NUT
C4R739I             EMPL     Removed on 07.298/17:26 by NUT
C4R739I             @TSD     Removed on 07.303/10:35 by ANUBIS
C4R739I             $U21AS  Added on 08.108/09:16 by OSIRIS
C4R739I  GrpAttr:  SPEC     @TSD     Removed on 07.303/10:31 by ANUBIS
C4R739I             @SECLSE  Removed on 07.303/11:22 by ANUBIS
C4R739I             OPER     @TSD     Removed on 07.303/10:31 by ANUBIS
```


Audit trail Example 2: LISTDSD

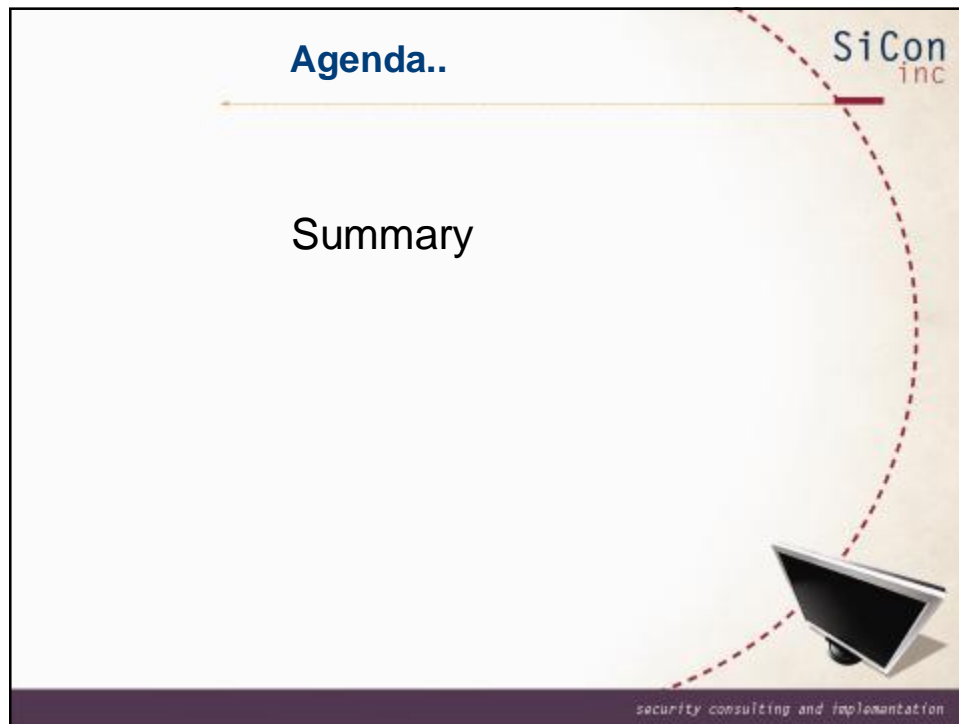


```
LISTDSD DA('HERA.**')
... Lines snipped ...
NO ENTRIES IN CONDITIONAL ACCESS LIST

C4R736I Command Audit Trail for DATASET  HERA.**
C4R739I  Attrib:  WARNING  Added on 08.072/11:07 by ZEUS
C4R739I             Removed on 08.072/11:07 by ZEUS
C4R739I  Access:  @SECLSE  access READ on 07.347/10:11 by AMANRA

C4R739I             FRED access READ on 08.093/08:56 by ISIS
```


security consulting and implementation

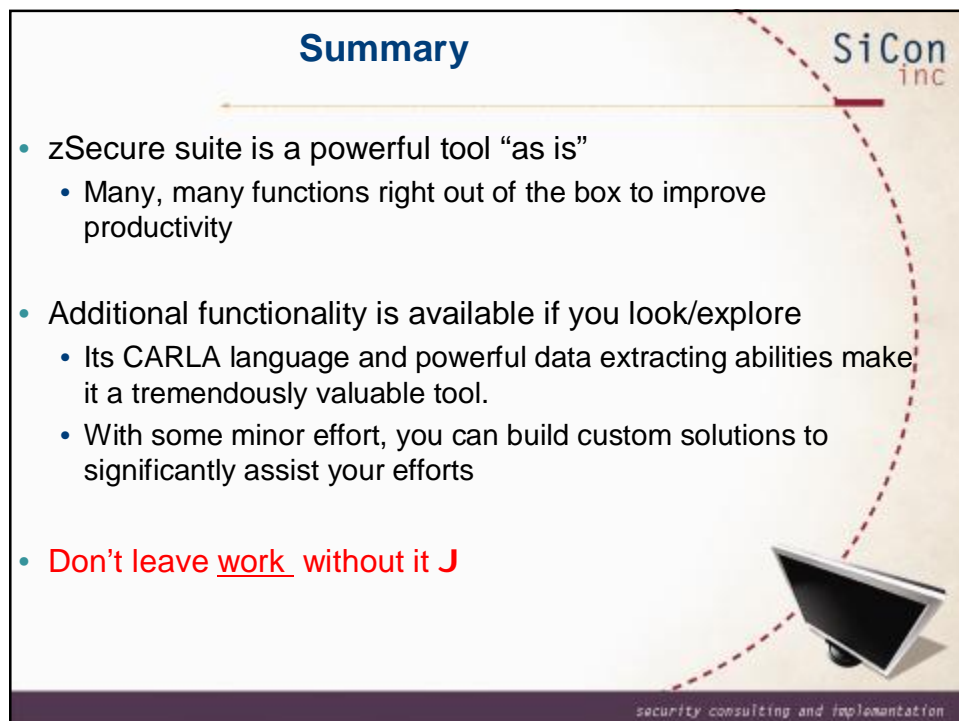


Agenda..

Summary

SiCon
inc

security consulting and implementation

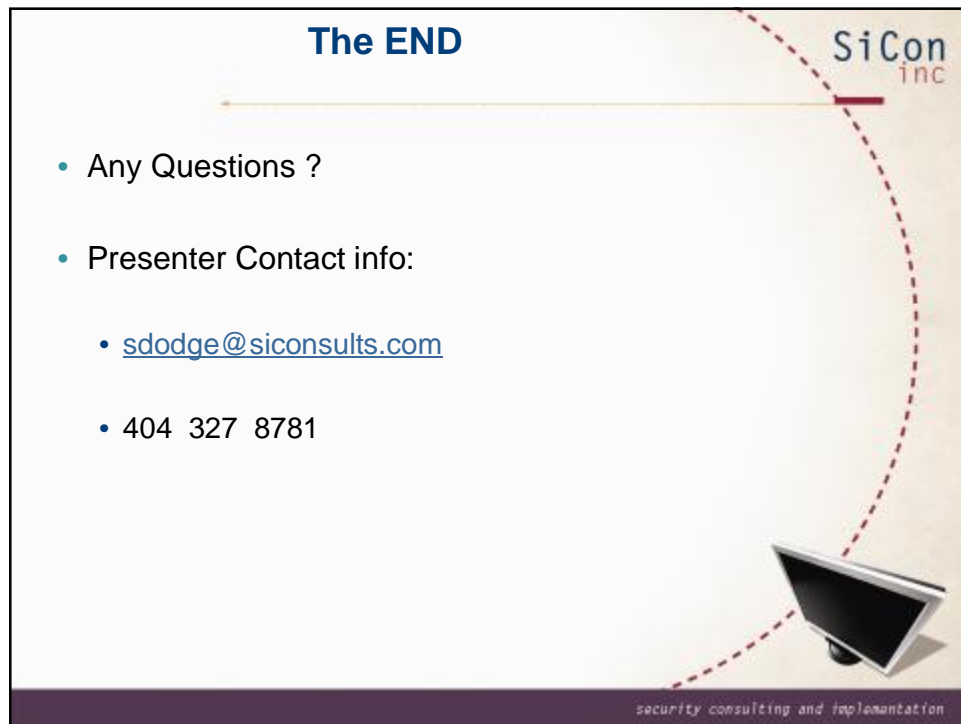


Summary

- zSecure suite is a powerful tool “as is”
 - Many, many functions right out of the box to improve productivity
- Additional functionality is available if you look/explore
 - Its CARLA language and powerful data extracting abilities make it a tremendously valuable tool.
 - With some minor effort, you can build custom solutions to significantly assist your efforts
- **Don't leave work without it J**

SiCon
inc

security consulting and implementation



The END

SiCon
inc

- Any Questions ?
- Presenter Contact info:
 - sdodge@siconsults.com
 - 404 327 8781

security consulting and implementation