Using CICS Security Discovery to adopt a zero-trust strategy

John D. Taylor
IBM Hursley

Notices and disclaimers

- © 2025 International Business Machines Corporation.
  All rights reserved.

- This document is distributed “as is” without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

- Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM.

- Not all offerings are available in every country in which IBM operates.

-

- Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

- IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: www.ibm.com/legal/copytrade.shtml.

- Certain comments made in this presentation may be characterized as forward looking under the Private Securities Litigation Reform Act of 1995.

- Forward-looking statements are based on the company’s current assumptions regarding future business and financial performance. Those statements by their nature address matters that are uncertain to different degrees and involve a number of factors that could cause actual results to differ materially. Additional information concerning these factors is contained in the Company’s filings with the SEC.

- Copies are available from the SEC, from the IBM website, or from IBM Investor Relations.

- Any forward-looking statement made during this presentation speaks only as of the date on which it is made. The company assumes no obligation to update or revise any forward-looking statements except as required by law; these charts and the associated remarks and comments are integrally related and are intended to be presented and understood together.

Research

IBM X-Force 2024 Report

71% increase of attacks using valid user credentials

85% of attacks on critical sectors could have been avoided by

- up-to-date fixes
- multi-factor authentication (MFA)
- least-privilege principles (Zero Trust!)

IBM Cost of data breach 2025 report
$4.4M global average cost of a data breach

https://newsroom.ibm.com/2024-02-21-IBM-Report-Identity-Comes-Under-Attack,-Straining-Enterprises-Recovery-Time-from-Breaches
https://www.ibm.com/reports/data-breach

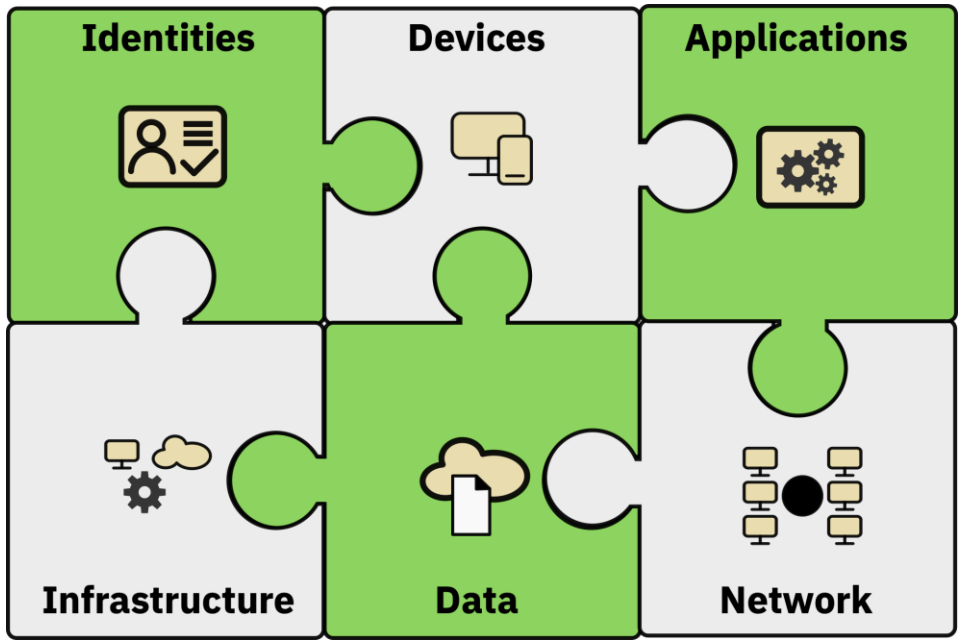
What is Zero Trust?

Focus on protecting resources not perimeters

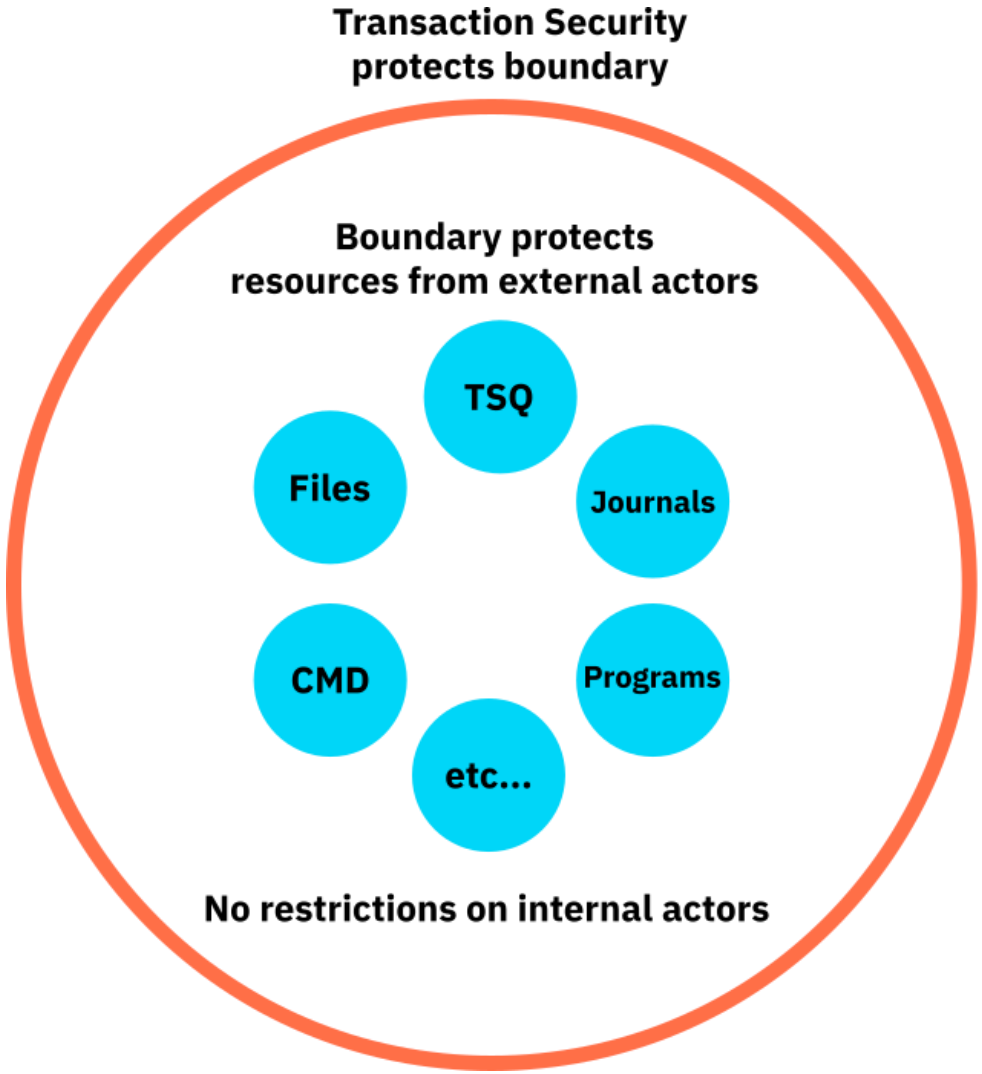
Enable the **right user,**
to have the **right access**,
to the **right data**,
for the **right reasons**.

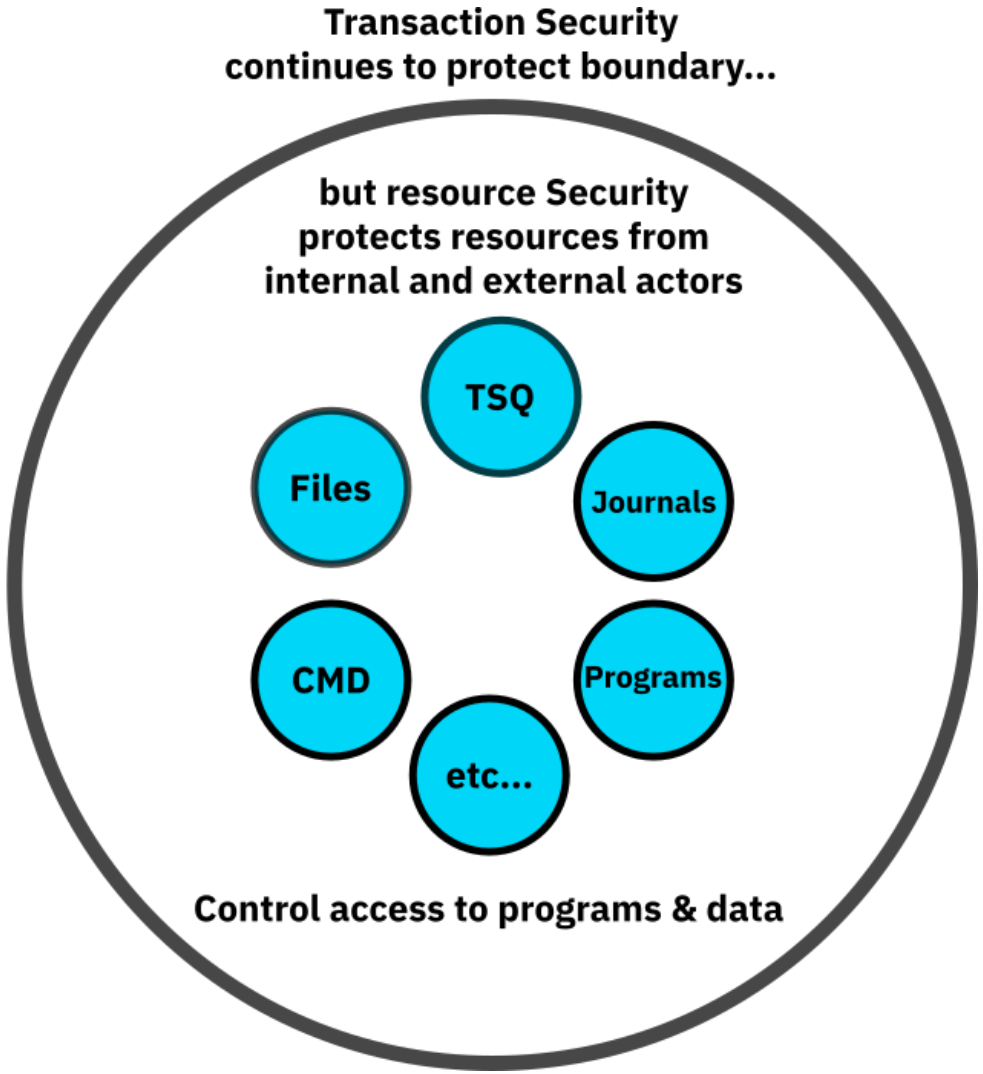
Never trust, always **verify**

Assume the bad actor is already present and **continuously monitor.**



CICS Transaction security is boundary security





Importance of Roles

Enable the right user,
to have the right access,
to the right data,
for the right reasons.

- A user's access should be related to their role
- Changing user access is as simple as adding them to a role or removing them from that role

Most customers either don't use roles, or use a mixture of roles and users

- Difficult to maintain
- Unused access often kept
- Very difficult to audit

Adoption workflow using the security discovery editor

Pre-reqs:

Production systems

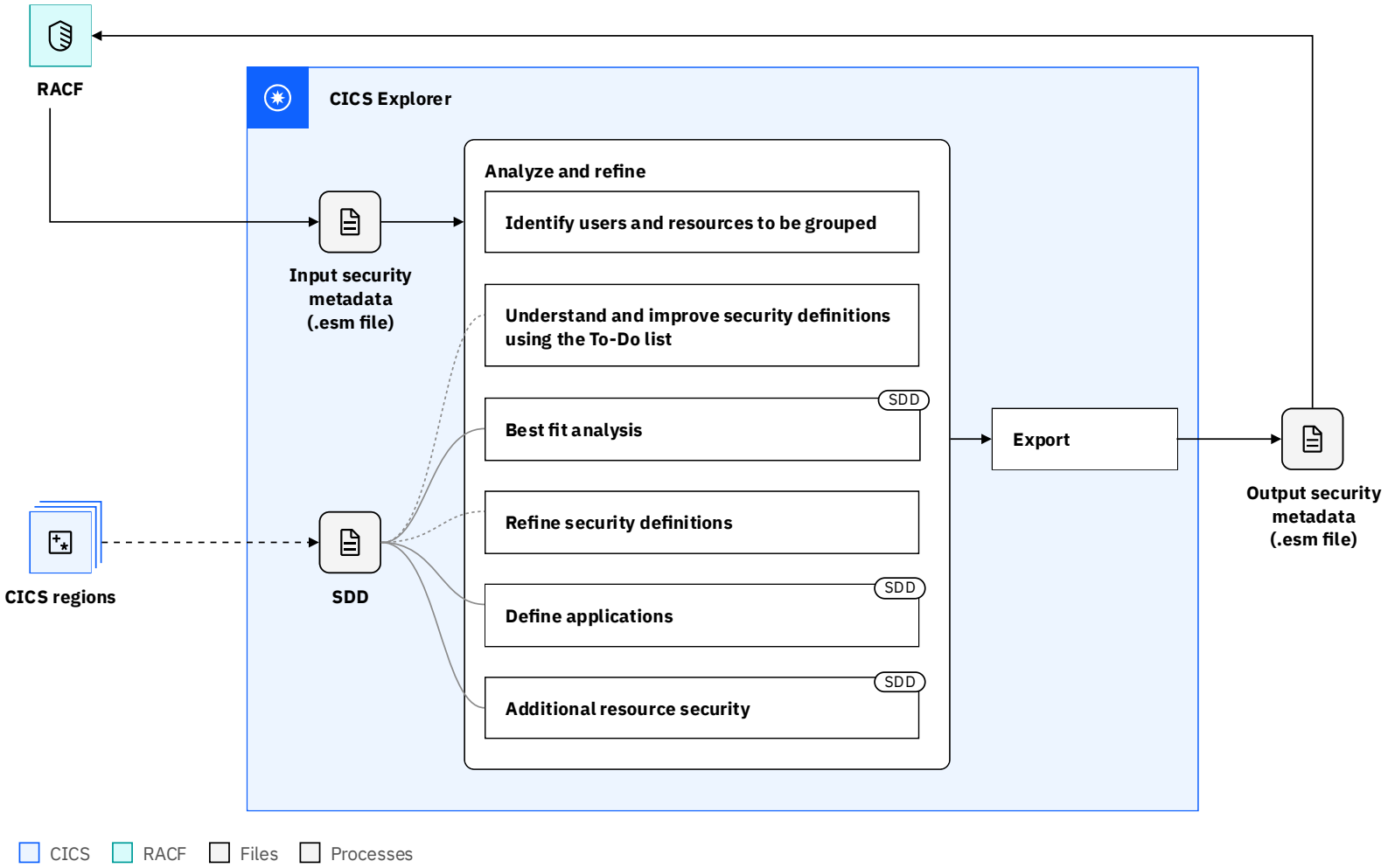
Security active

Transaction security enabled

Move from an ad-hoc evolved security model to a manageable, resilient set of definitions for transaction security, and...

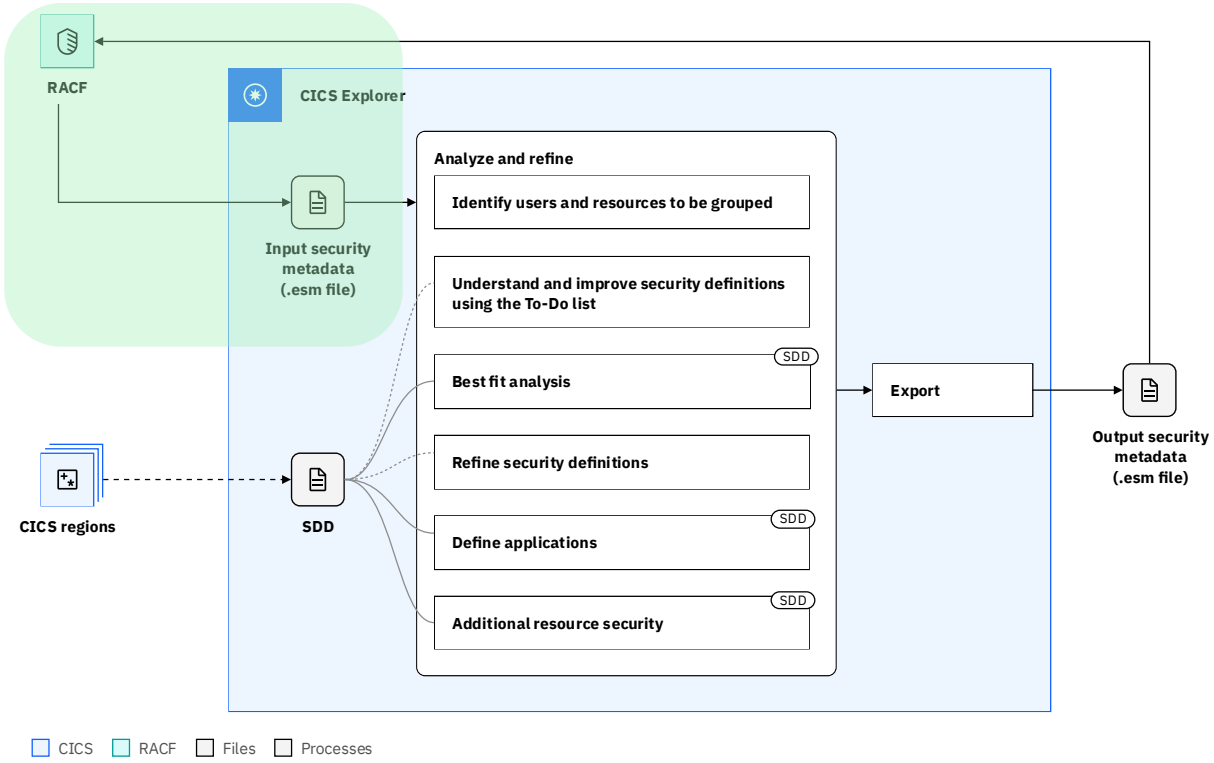
adopt and extend the model to other CICS resources for security in depth

CICS Security Discovery



1. Extract RACF definitions
2. Review and action To-dos for security definitions in CICS Explorer and export them for review
3. Create RACF commands from reviewed security definitions
4. Capture security discovery data (SDD). This can be done in parallel with steps 1 through 3.
5. Check and refine definitions using SDD observed behavior
6. Adopt and extend transaction security model to other resource types
7. Create RACF commands from reviewed security definitions

Import RACF definitions as security metadata



- Imports transaction class and groups using this class
- Assumes users have good transaction security
- Separate import for each SECPRFX
- Optionally imports other CICS security classes

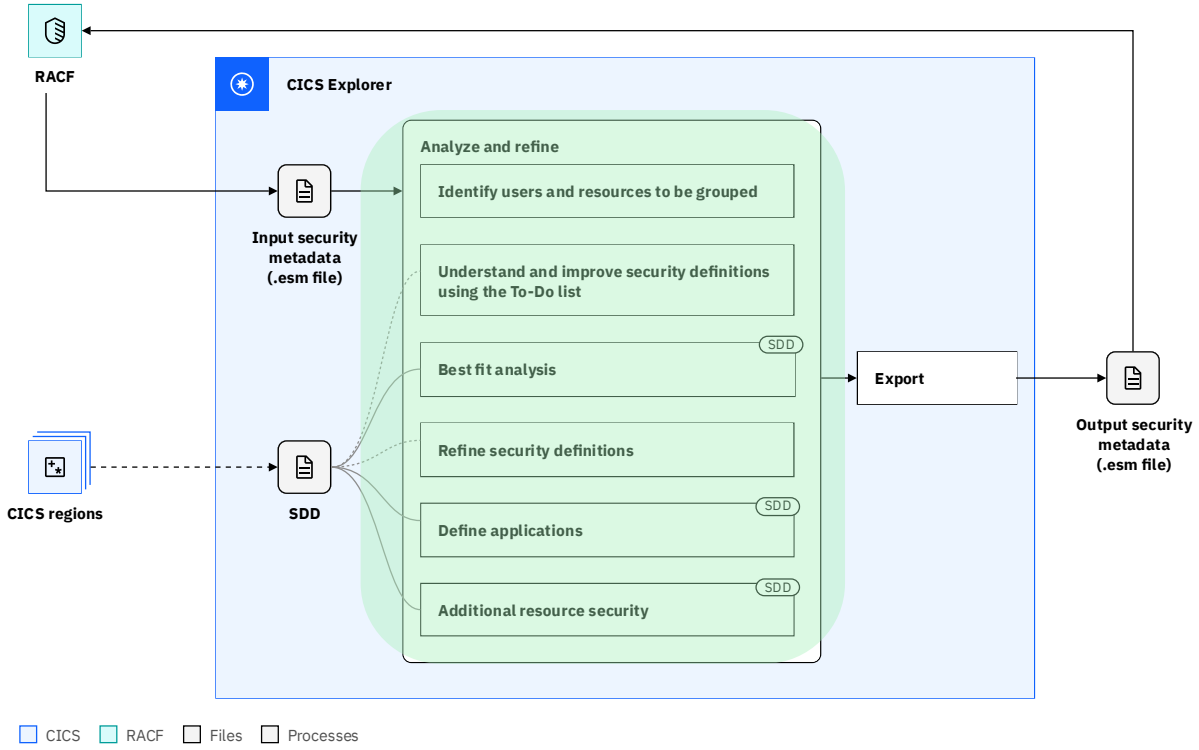
DFH$R2SM

```
//SECMETA JOB
//SECMETA  EXEC DFHXSMET,SAMPLIB=hlq.SDFHSAMP,
//      DIR='/u/userid/cics/', FN='regionsA'
//INPUT.SYSIN DD *
XTRAN=CICSTRN
SECPRFX=NO
//
```

Security metadata

```
--- # Security Metadata ---
version: 2
file_created:
  - date: "17 Mar 2023"
  - time: "17:27:26"
  - user: SUE
group_list:
  - name: MANAGER
    users:
      - MAINWRN
  - name: TELLER
    users:
      - WILSON
      - PIKE
user_list:
  - user: JONES
    username: "Jack Jones"
  - user: MAINWRN
    username: "George Mainwaring"
  - user: PIKE
    username: "Frank Pike"
  - user: WILSON
    username: "Arthur Wilson"
secprfx: NO
classes:
  - class: XTRAN
    name: CICSTRN
    profiles:
      - name: BANKING
        members:
          - BNK1
          - BNK2
        access_lists:
          - access: READ
            groups:
              - MANAGER
              - TELLER
            users:
              - JONES
```

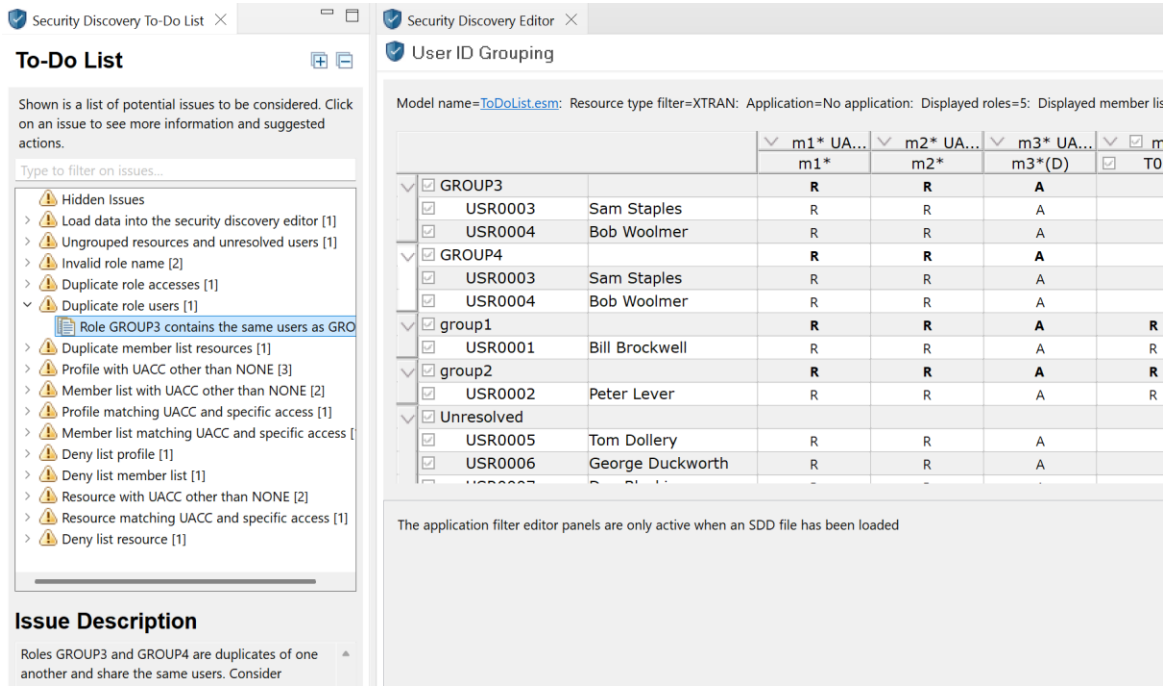
Analyse security definitions in CICS Explorer



Use security metadata to

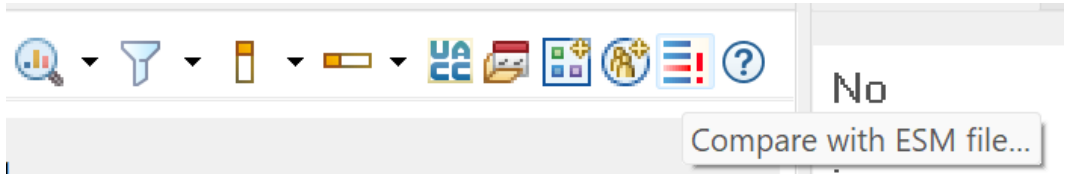
- Identify areas where existing definitions do not match best practice or zero trust objectives
- Improve existing definitions and move to better role-based access controls

- CICS Explorer - Security Discovery Perspective
  - Table shows current definitions
  - To-do list highlights areas for improvement

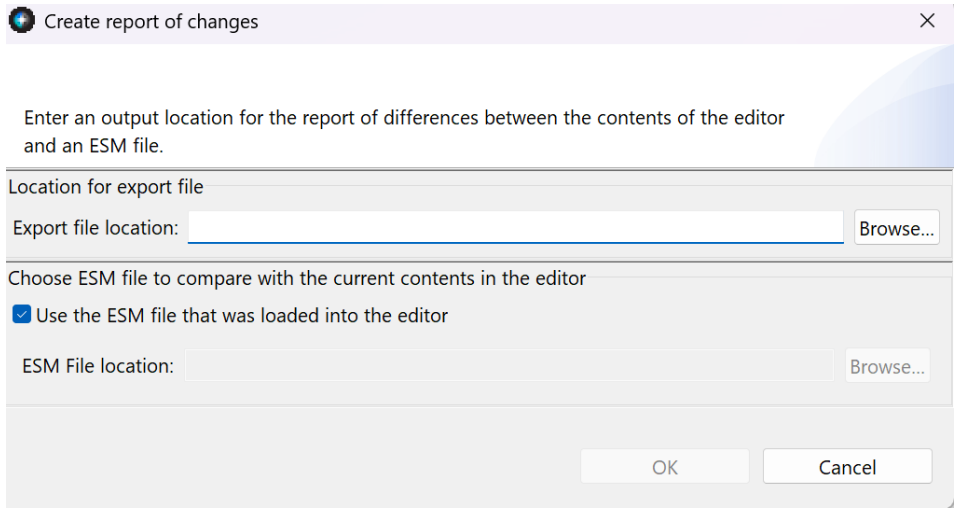


Compare changes with the ESM file…

Action on the toolbar ‘Compare with ESM file…



Specify a location for the output report
Either compare with the originally loaded ESM file, or specify a different ESM file…



Security discovery editor comparison report
Report generated: <date-time>
Report for file: <ESM file name>
.
.
.
Roles added:
Role
g000
g001
.
.
.
Users added to roles
User Role
USR0024 g000
USR0158 g000
.
.
.
Users gained accesses

User	Resource	Old-access	New-access
USR0003	XTRAN.T026	NONE	R
USR0003	XTRAN.T050	NONE	R

.
.
.
etc…

Demo 1
(Using just the ESM file from RACF)

Capturing Security Discovery Data

Requires CICS v6.2 or later

Discovers resources used based on
- Userid
- Transaction
- Origin transaction

Each access only captured once
- Each level of access recorded

Data captured in 64-bit memory

Long running process

Small performance overhead

Activated by PLT or CICS Explorer

Captures CICS security accesses
- Ignores Xnnn settings
- Ignores RESSEC/CMDSEC setting

Data written daily to a logstream
- Also, at shutdown or on request

Data for sets of regions combined offline

SDD: SPI for SECDISCOVERY

- Start/stop collecting data for all or selected classes

```
SET SECDISCOVERY

 < STATUS() | ON | OFF >
 < DISCOVERALL | _classes_ >
```

- Status of data collection
- Transaction data always collected
- Information about how much data is being collected

```
INQUIRE SECDISCOVERY

 < STATUS() >
 < TRAN() > _classes_
 < LASTSECDTIME() > < LASTWRITTIME() >
 < SECDCOUNT() > < NEWSECDCOUNT() >
```

- Write data out

```
PERFORM SECDISCOVERY WRITE
```

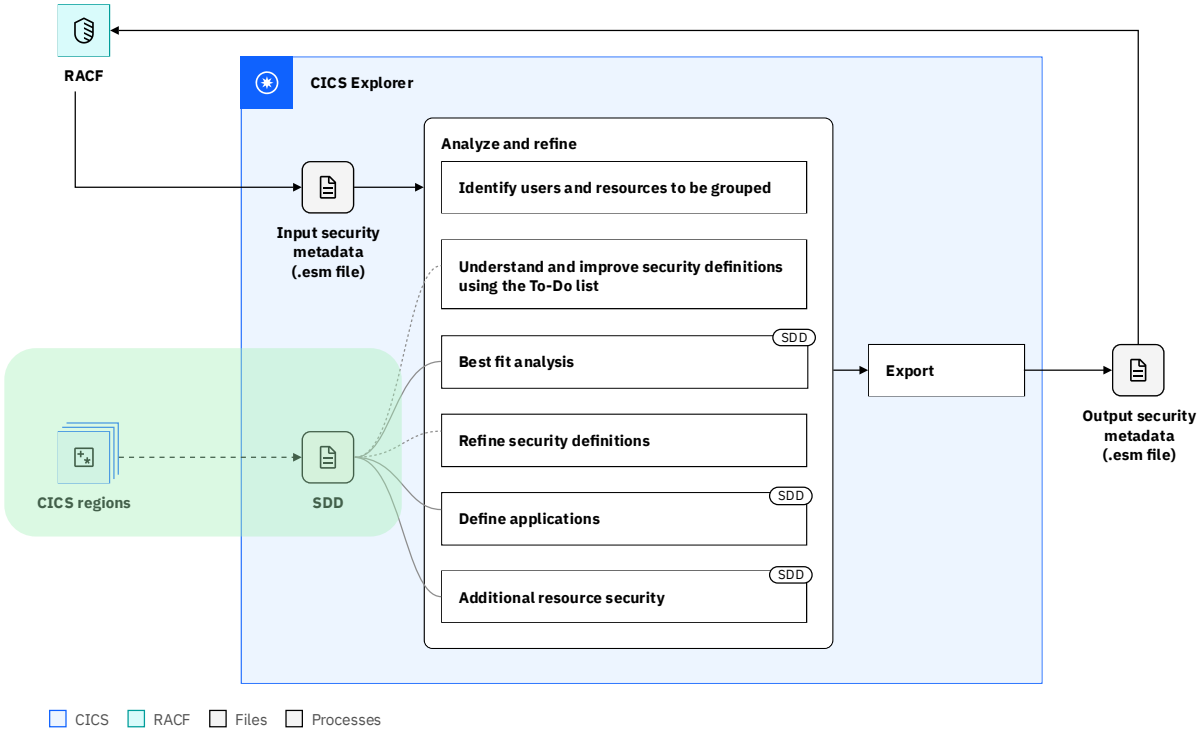
SDD: How much data to capture?

Expect to be left running for an extended period

- Capture normal use and special periods (end of month, year etc.)
- Stats to show how much data is being collected
- Data collection should tail off after a few days
- Also available with CICS Explorer and SPI

- DFHXS1602 date time applid Security Discovery is {active|inactive}. Total records: recordcount. Records since last write: writecount. Last recording: mm/dd/yyrecorddate hh:mm:ssrecordtime. Last write: mm/dd/yywritedate hh:mm:sswritetime.

Capture security discovery data (SDD)



- Switch on SECDISCOVERY to capture usage data
  Data in memory, written out to logstream once a day
- Message DFHXS1602 shows new data captured each day
- When very little new data create SDD file

- System programming interface (SPI)

```
SET SECDISCOVERY

 < STATUS() | ON | OFF >
 < DISCOVERALL | _classes_ >

INQUIRE SECDISCOVERY

 < STATUS() >
 < TRAN() > _classes_
 < LASTSECDTIME() > < LASTWRITTIME() >
 < SECDCOUNT() > < NEWSECDCOUNT() >

PERFORM SECDISCOVERY WRITE
```

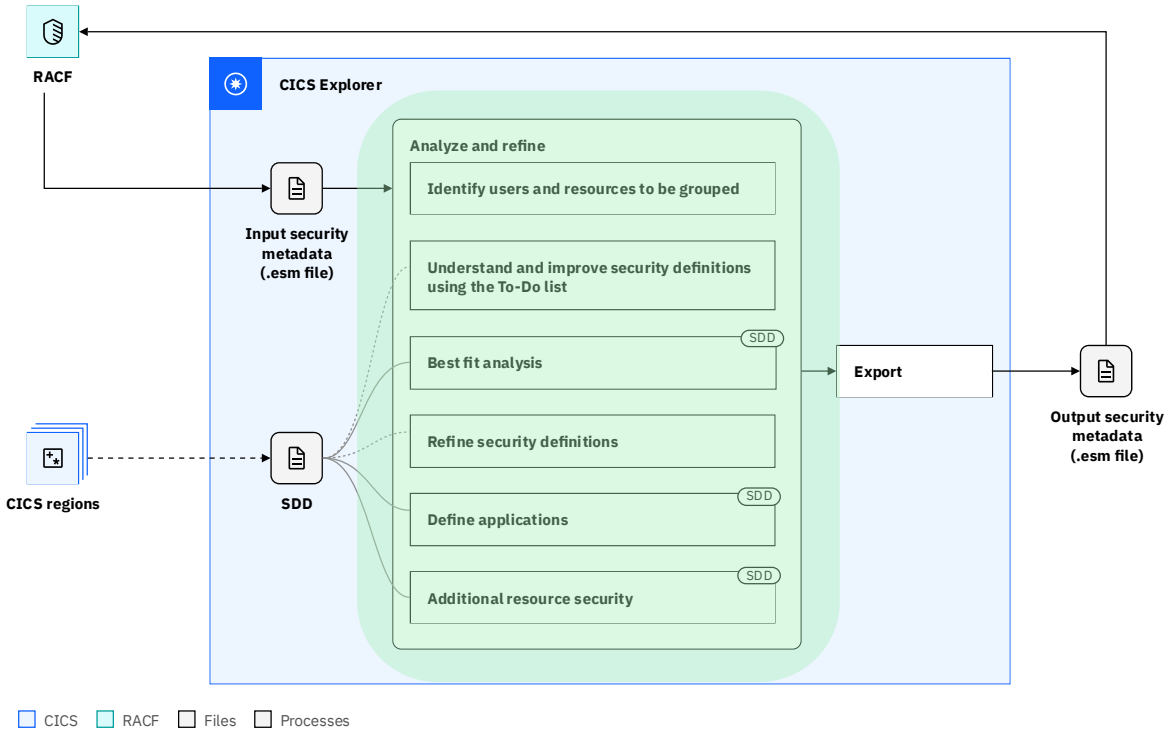
- DFH$SDDP

```
//SECDSDD JOB
...
//SDD      EXEC PGM=DFHSDD
//STEPLIB  DD DISP=SHR,DSN=&HLQ..SDFHLINK
//DFHSECD  DD other definitions,DSNAME=&LOGSTRM
//DFHSDD   DD other definitions,PATH='&SDD'
...
```

- SDD

```
userid,principal,session,region,default,resource type,class,profile,max
access,READ,UPDATE,CONTROL,ALTER,INQUIRE,SET,COLLECT,PERFORM,EXECUTE,CREATE,DISCARD,DEFINE,INSTALL,START,SUBM
IT,DELETE,SET_CONTROL,SET_ALTER,QUERYU0000001,Y,N,N,N,TRANSATTACH,TCICSTRN,T002,READ,N,N,N,N,N,N,N,N,Y,N,N,N,
N,N,N,N,N,NU0000001,Y,N,N,N,TRANSATTACH,TCICSTRN,T009,READ,N,N,N,N,N,N,N,Y,N,N,N,N,N,N,N,N,NU0000002,Y,
N,N,N,TRANSATTACH,TCICSTRN,T001,READ,N,N,N,N,N,N,N,Y,N,N,N,N,N,N,N,N,NU0000002,Y,N,N,N,TRANSATTACH,TCICST
RN,T002,READ,N,N,N,N,N,N,N,N,Y,N,N,N,N,N,N,N,N,NU0000003,Y,N,N,N,TRANSATTACH,TCICSTRN,T004,READ,N,N,N,N,N,N
,N,N,Y,N,N,N,N,N,N,N,N,NU0000003,Y,N,N,N,TRANSATTACH,TCICSTRN,T005,READ,N,N,N,N,N,N,N,Y,N,N,N,N,N,N,N,N
,N
```

Analyse security definitions in CICS Explorer



- CICS Explorer - Security Discovery Perspective

			trn000				
			T001	T002	T003	T004	T005
	USR0192	Jack Russell					
	USR0197	Damien Martyn					
	USR0216	David Hookes					
	USR0238	Tom Curran					
g001			**Rr**	**R+r**	**R+r**	**Rr**	**Rr**
	USR0064	Arthur Mold	R	Rr	R	Rr	Rr
	USR0087	Dean Jones	Rr	R	R+	R	Rr
	USR0105	Syd Gregory	Rr	R	R	Rr	R
	USR0199	Archie MacLaren	Rr	Rr	Rr	Rr	Rr
	USR0209	Eoin Morgan	Rr	Rr	Rr	Rr	Rr
	USR0235	Johnny Taylor	Rr	Rr	Rr	Rr	Rr
	USR0263	Bob Woolmer	Rr	R	Rr	Rr	Rr
	USR0281	Kevin Pietersen	Rr	R+	Rr	Rr	Rr
g002							
	USR0123	Paul Allott					
	USR0154	Don Wilson					
g003							
	USR0015	Andrew McDonald					
g004							
	USR0024	Roland Pope					

Use Security Discovery Data to

- Validate current permissions against actual usage
- Check and refine user groups and transaction member lists
- Create user groups with access to other resource member lists

Migrating to Resource Security

We think most customers do not currently have:

- Fully automated application tests
- Good coverage of manual tests
- Security testing (manual or automated)

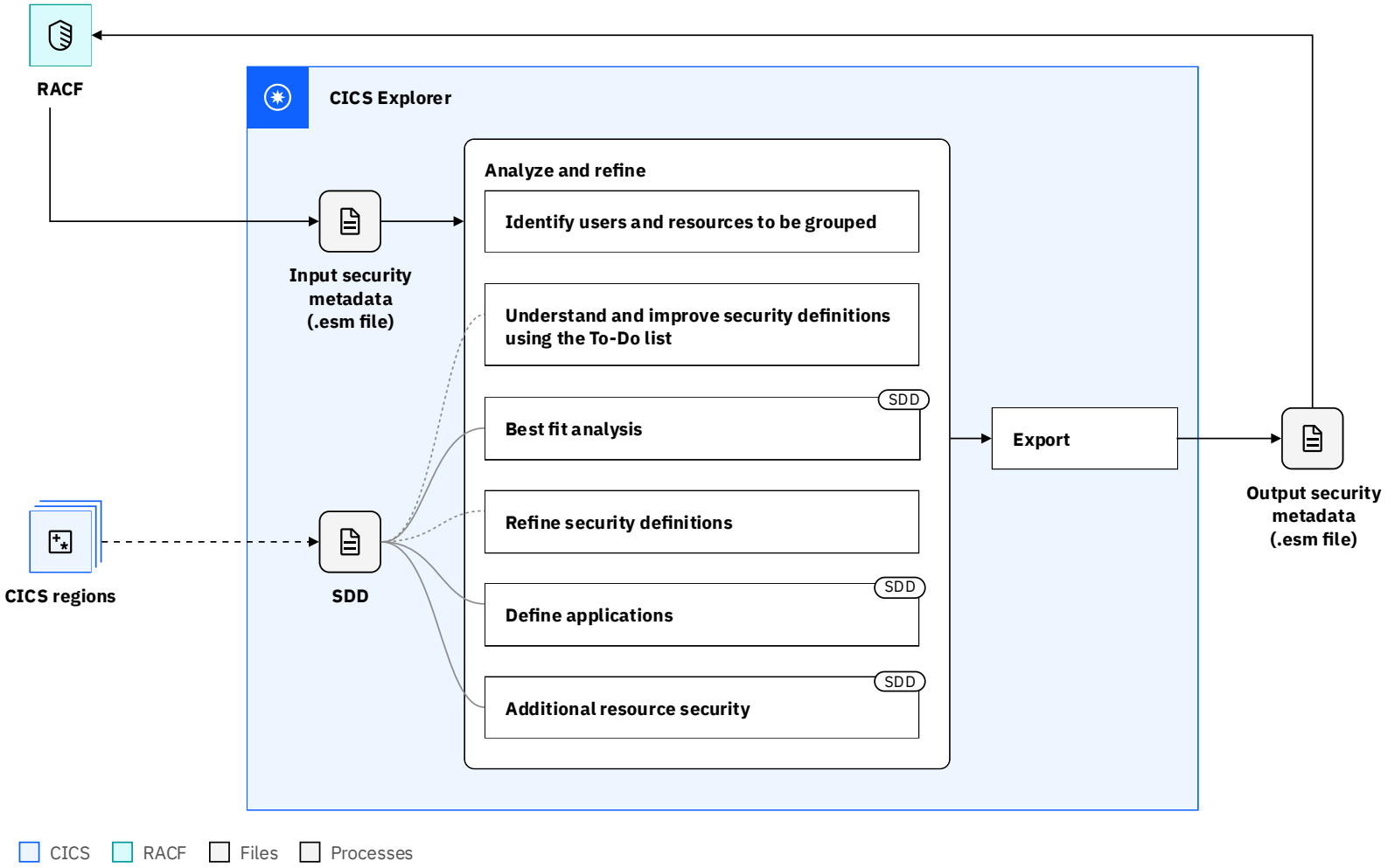
How do you decide which roles to create?

What access should each role have?

Migrating without breaking our mission critical applications!

Demo 2
(Using the CICS Security Discovery Data file)

Summary of the steps



1. Extract RACF definitions
2. Review and action To-dos for security definitions in CICS Explorer and export them for review
3. Refine security definitions
4. Create RACF commands from reviewed security definitions
5. Capture security discovery data (SDD). This can be done in parallel with steps 1 through 4.
6. Check and refine definitions using SDD observed behavior
7. Adopt and extend transaction security model to other resource types
8. Create RACF commands from reviewed security definitions

Review of Demos

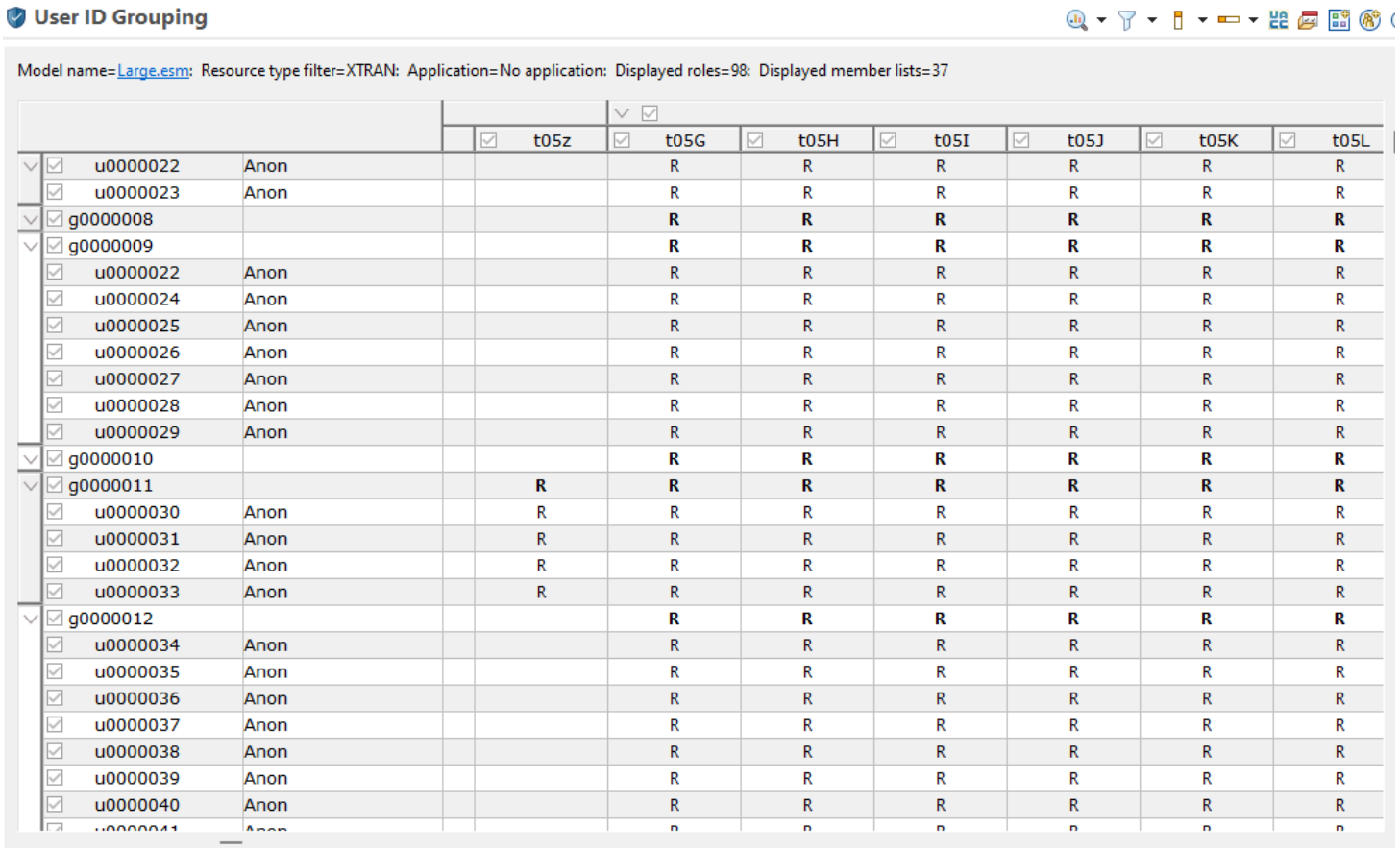
Uses CICS Explorer 5.5.46 (34.0.6) or later
- Download from Download site

Demo 1: Uses data extracted from RACF
- JCL available with CICS v6.1 and above
- The ESM file

Demo 2: Uses CICS security discovery data
- requires CICS v6.2 or later
- The SDD file

ESM review

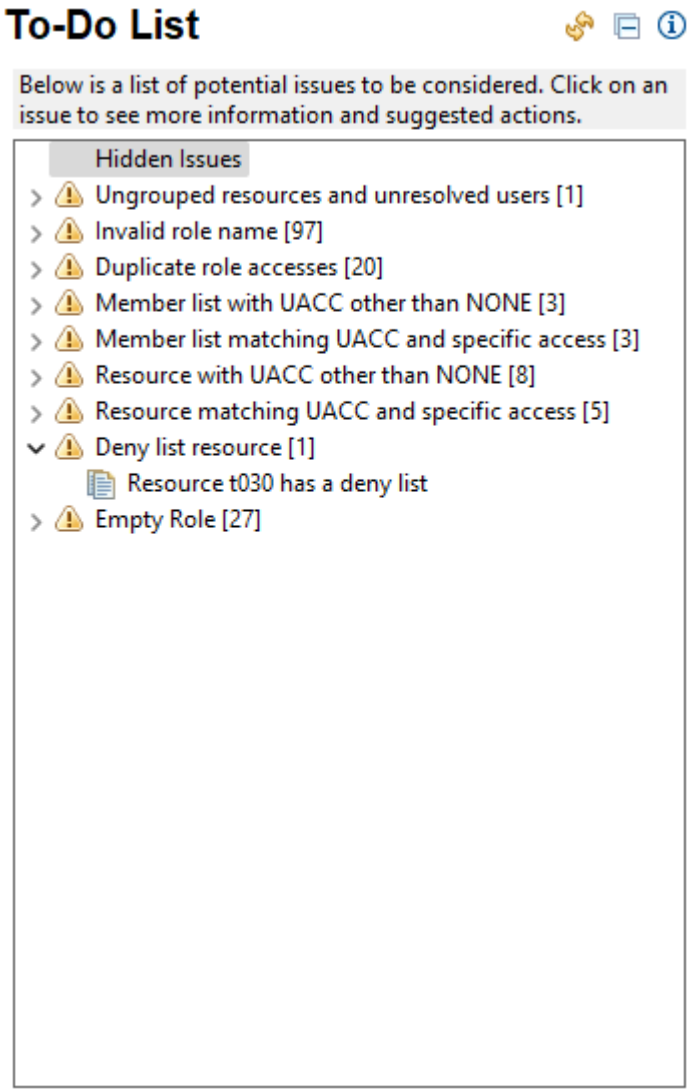
Loaded RACF data into the explorer (the ESM file)



		t05z	t05G	t05H	t05I	t05J	t05K	t05L
u0000022	Anon		R	R	R	R	R	R
u0000023	Anon		R	R	R	R	R	R
g0000008			**R**	**R**	**R**	**R**	**R**	**R**
g0000009			**R**	**R**	**R**	**R**	**R**	**R**
u0000022	Anon		R	R	R	R	R	R
u0000024	Anon		R	R	R	R	R	R
u0000025	Anon		R	R	R	R	R	R
u0000026	Anon		R	R	R	R	R	R
u0000027	Anon		R	R	R	R	R	R
u0000028	Anon		R	R	R	R	R	R
u0000029	Anon		R	R	R	R	R	R
g0000010			**R**	**R**	**R**	**R**	**R**	**R**
g0000011		**R**	**R**	**R**	**R**	**R**	**R**	**R**
u0000030	Anon	R	R	R	R	R	R	R
u0000031	Anon	R	R	R	R	R	R	R
u0000032	Anon	R	R	R	R	R	R	R
u0000033	Anon	R	R	R	R	R	R	R
g0000012			**R**	**R**	**R**	**R**	**R**	**R**
u0000034	Anon		R	R	R	R	R	R
u0000035	Anon		R	R	R	R	R	R
u0000036	Anon		R	R	R	R	R	R
u0000037	Anon		R	R	R	R	R	R
u0000038	Anon		R	R	R	R	R	R
u0000039	Anon		R	R	R	R	R	R
u0000040	Anon		R	R	R	R	R	R

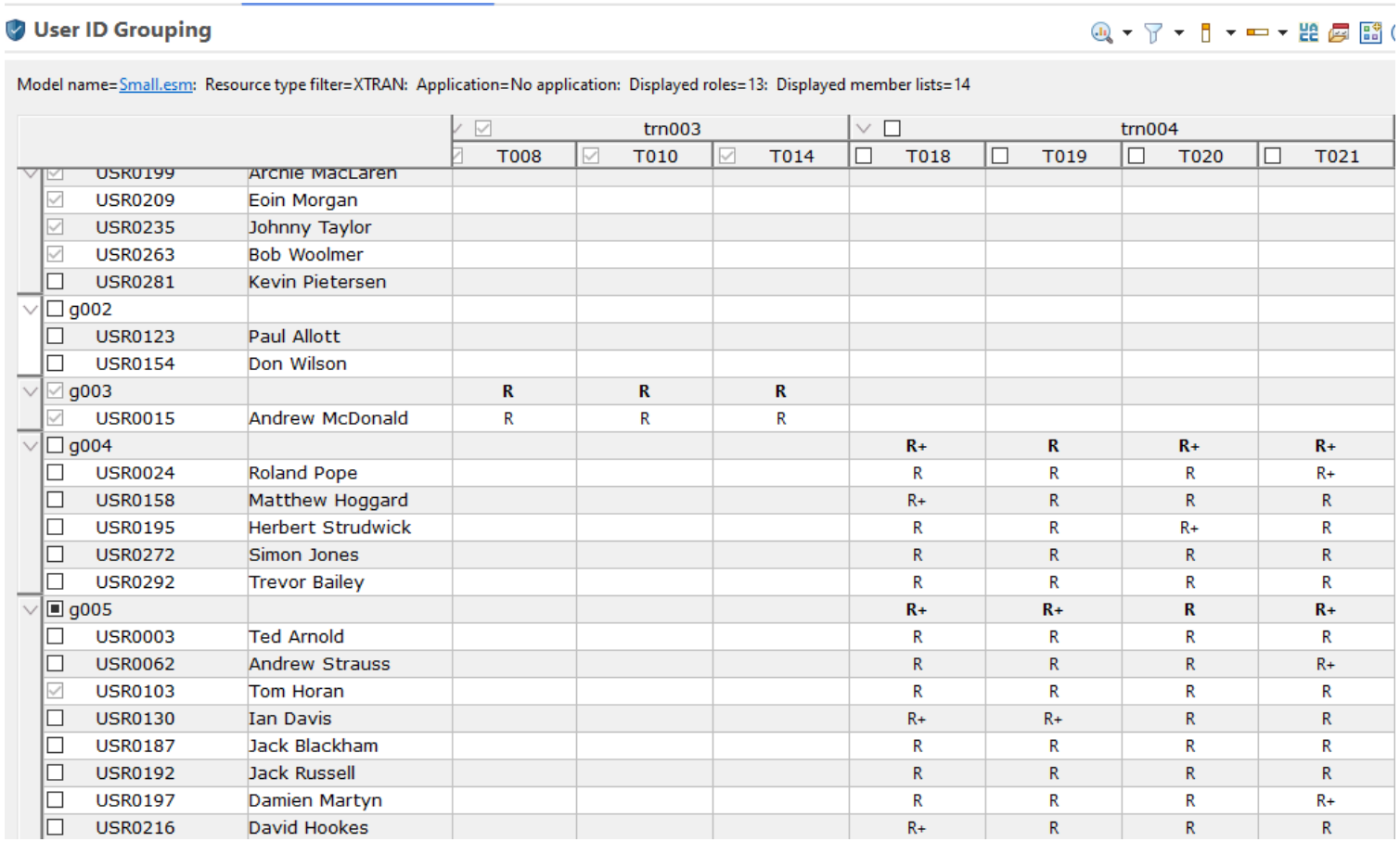
Todo list

We looked at the new To-Do list



Analyse

The data were analysed and changed as required



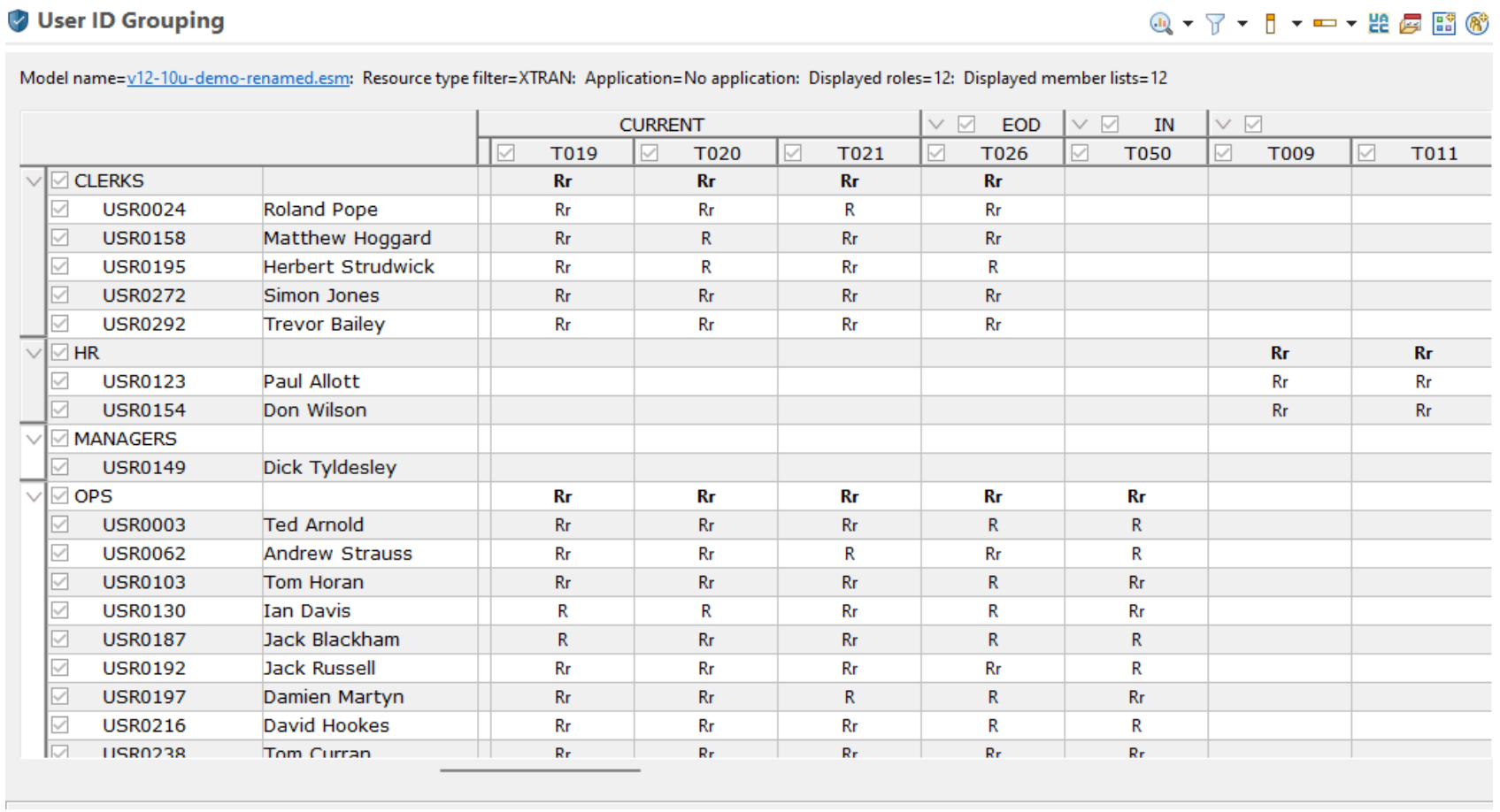
User ID Grouping

Model name=Small.esm: Resource type filter=XTRAN: Application=No application: Displayed roles=13: Displayed member lists=14

		trn003			trn004			
		T008	T010	T014	T018	T019	T020	T021
USR0199	Archie MacLaren							
USR0209	Eoin Morgan							
USR0235	Johnny Taylor							
USR0263	Bob Woolmer							
USR0281	Kevin Pietersen							
g002								
USR0123	Paul Allott							
USR0154	Don Wilson							
g003		**R**	**R**	**R**				
USR0015	Andrew McDonald	R	R	R				
g004					**R+**	**R**	**R+**	**R+**
USR0024	Roland Pope				R	R	R	R+
USR0158	Matthew Hoggard				R+	R	R	R
USR0195	Herbert Strudwick				R	R	R+	R
USR0272	Simon Jones				R	R	R	R
USR0292	Trevor Bailey				R	R	R	R
g005					**R+**	**R+**	**R**	**R+**
USR0003	Ted Arnold				R	R	R	R
USR0062	Andrew Strauss				R	R	R	R+
USR0103	Tom Horan				R	R	R	R
USR0130	Ian Davis				R+	R+	R	R
USR0187	Jack Blackham				R	R	R	R
USR0192	Jack Russell				R	R	R	R
USR0197	Damien Martyn				R	R	R	R+
USR0216	David Hookes				R+	R	R	R

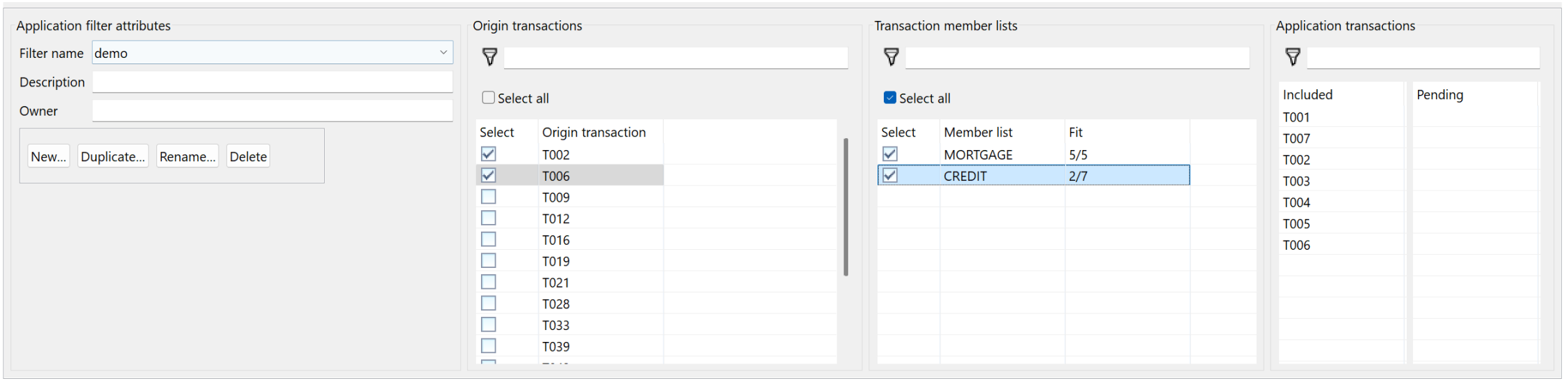
Used SDD data

CICS SDD data file loaded and used to get more information



Define an application filter

Used the application filter panel



Create security definitions for Files

Best fit analysis against application filtered data

Model name=v12-10u demo-part2(2).esm: Resource type filter=XFCT: Application=demo: Displayed roles=14: Displayed member lists=5: Hidden ungrouped resources=38

		fct000	fct001		fct002			fct003		fct004
		FI0004	FI0005	FI0007	FI0008	FI0009	FI0010	FI0001	FI0002	FI0003
OTHERS										
USR0042	George Studd									
USR0099	Kurtis Patterson									
USR0243	Bill Johnston									
USR0256	Ernie Hayes									
USR0293	Tom Hogan									
OTHERS_XFCT+r		**R+r**			**R+r**	**R+r**	**R+r**			
USR0042	George Studd	R+r			R+r	R+r	R+r			
OTHERS_XFCT+u		**U+u**	**U+u**	**U+u**						
USR0042	George Studd	U+u	U+u	U+u						
SYSPROGS										
USR0003	Ted Arnold									

Summary

- The zero-trust journey can be difficult
  - Understanding what you currently have defined in RACF
  - Knowing what to change without breaking key applications or job roles
- Using ESM and SDD in the new Explorer can help a lot
  - Refining ESM data helps in the organisation of security definitions overall
  - SDD data lets actual usage of resources be accounted for in security definitions
    - Enables required security access permissions to be assessed before changes are made to the security definitions

Give it a try for almost no effort...

1. Capture the ESM data from your own RACF
2. Load the ESM data into your CICS Explorer 5.5.46 (34.0.6) or later
3. See what is called out in the To-do list. Either:
   a. Be smug about how good everything looks, or
   b. Look at what can be better and consider making improvements to make your life easier
4. Come back and tell us about what you found out!

   Just share your to-do list?

   Use the JCL to anonymize your data and share the whole editor?

Thank you for your attention

Any questions?