# SHARE Winter 2026 – Orlando, FL

SHARE
EDUCATE • NETWORK • INFLUENCE

## Security Discovery in CICS

**Lewis James**
CICS TS for z/OS Development
IBM UK

# IBM X-Force Research 2025

Know your threats…

**30%**

Abusing valid accounts remained the preferred entry point into victim environments for cybercriminals in 2024, representing 30% of all incidents X-Force responded to.

**84%**

Phishing emerged as a 'shadow' infection vector for identity attacks. While the share of successful phishing compromises has dropped by nearly 50% since 2022, X-Force observed an 84% uptick in phishing emails delivering infostealers on a weekly basis.

**25%**

Attackers exploited vulnerabilities in more than one-quarter of incidents X-Force responded to across critical sectors last year, with outdated systems and slow patching cycles proving to be an enduring challenge

# When the auditor comes knocking…

Auditors inspecting security environments are looking at key compliance with industry standard regulations

EU

GDPR

DORA

NIS2

US

HIPAA

SOX

ISO

PCI-DSS

# Complying with the regulations

It is easier said than done in ‘just complying’ with the regulations.

Large international corporations may be required to comply with multiple security regulations when

- The corporation has a presence within multiple geographies
- A national corp serving international customers handling and storing their PI

A common framework or strategy is required in centralizing the approach of cyber security

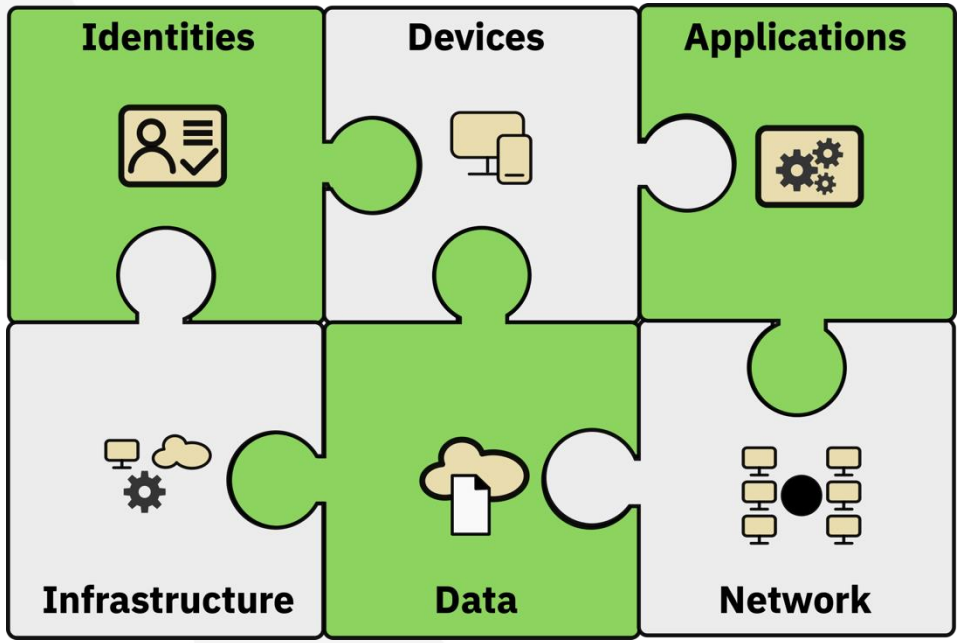
# What is Zero Trust

Focus on protecting resources not perimeters

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

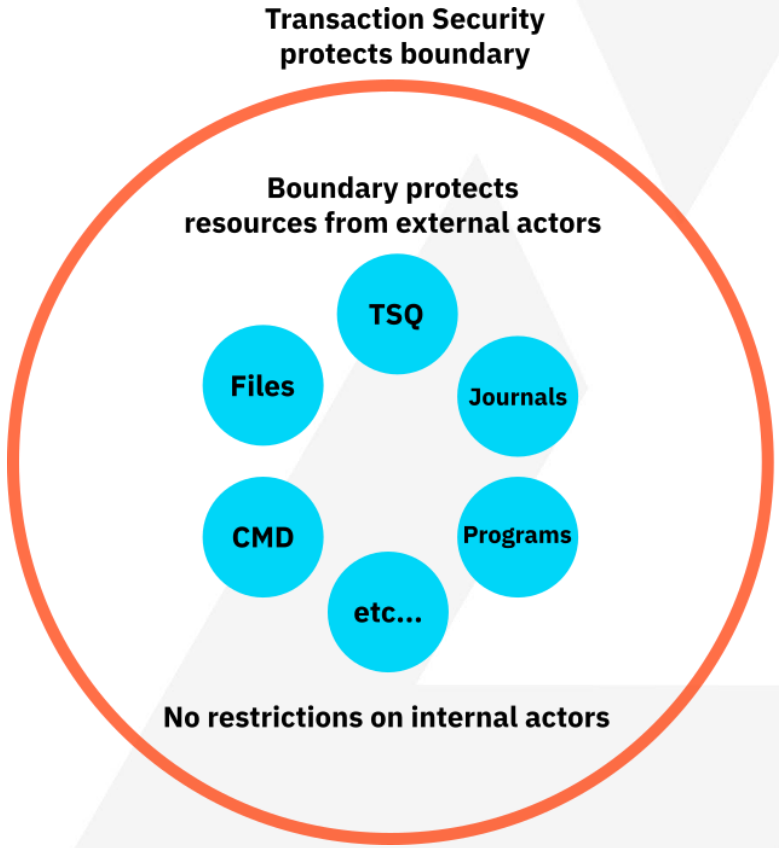
Never trust, always verify

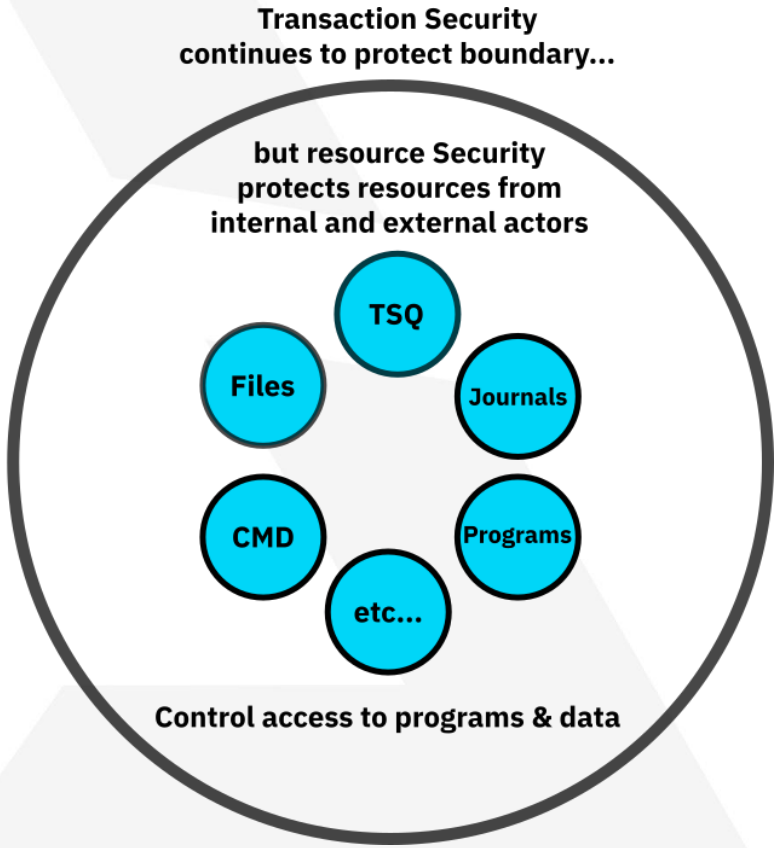
Assume the bad actor is already present and continuously monitor.



# CICS Transaction Security (XTRAN)

CICS transaction security enabled with XTRAN is a form of boundary security



# Common Environment Security

From research we know that a good majority of customers will run with transaction security, but a minority have implemented effective resource checks

- All production systems will have XTRAN active
- Some may have XUSER & XCMD active
- Very few have other security classes active
- Most transactions have CMDSEC(NO) RESSEC(NO)
- All system access uses the CICS region user ID

There are significant challenges in changing this

# Enabling Resource Security

The challenges with ‘just switching on’ resource security are extensive

- How do you approach the task
- There is a lack of information
- Complexity due to large number of users and differing accesses
- Cost of the increased security checks

Traditionally, there has been a black hole where support and guidance is expected.

# Importance of Roles

SHARE
EDUCATE • NETWORK • INFLUENCE

" 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 a user's access becomes as simple as moving them from one role to another

If only it was that easy… ☺

- Most customers use a mix of user and role-based security – unorganized and complex

# Introducing Security Discovery

CICS security discovery is a tool introduced in CICS Transaction Server 6.2

Designed to directly eliminate the challenges in enabling resource-based security

- Improve maintainability
- Improve security
- Reduce administration overhead
- Cost estimation of additional security checks

Making the essential jump to beyond traditional boundary security

# Security Discovery

Security Discovery enables the capturing of two essential pieces of data

**Security Discovery Data (SDD)**

**SET SECDISCOVERY**

Enabled in production for an extended period.

Capture security accesses that have *or would have* occurred.

Outputs to log stream.

Export to unix .SDD file.

**Export RACF DB**

JCL provided at CICS Transaction Server 6.1.

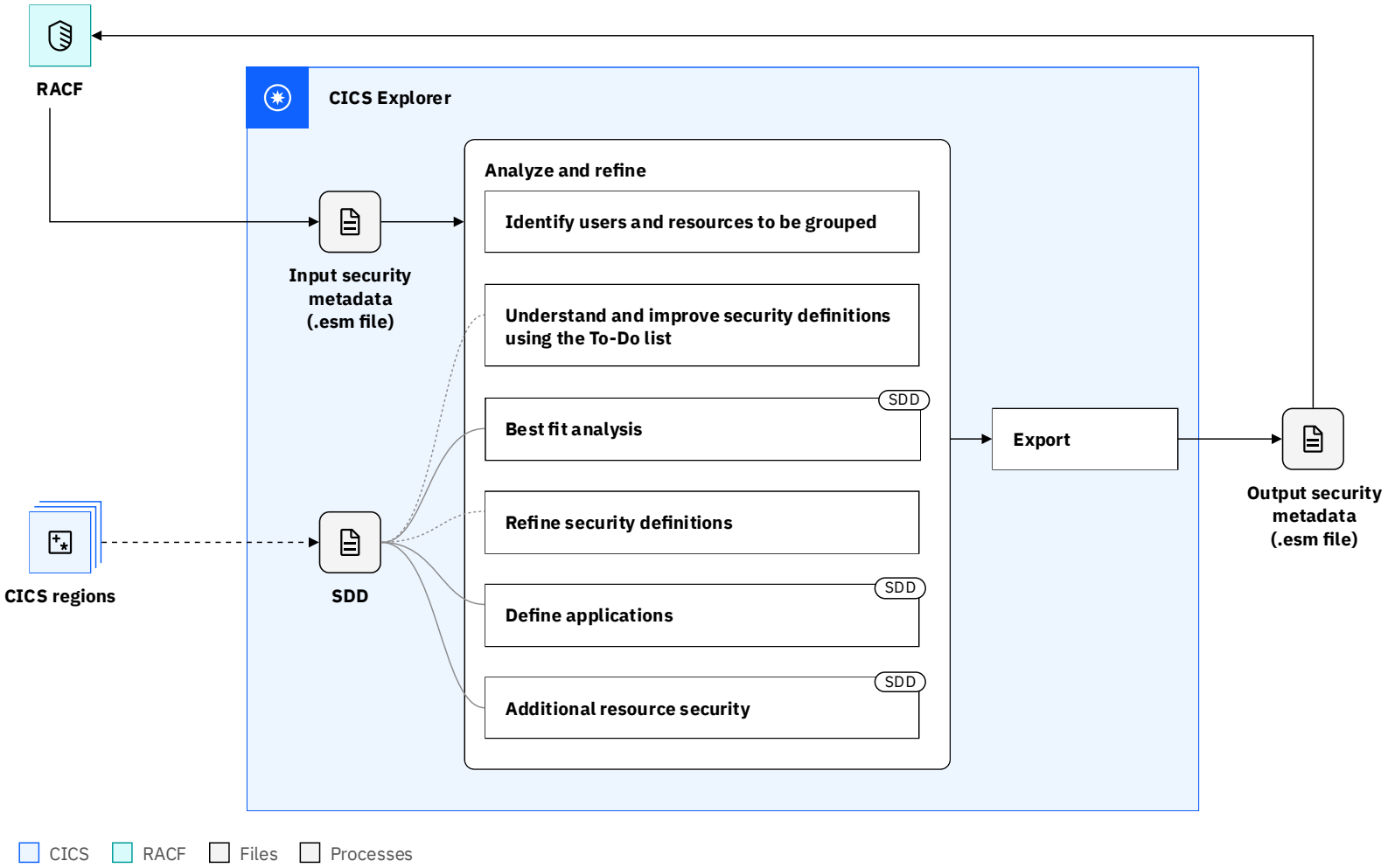
Import transaction class and groups.

Imports all CICS security classes.

Controlled YAML format

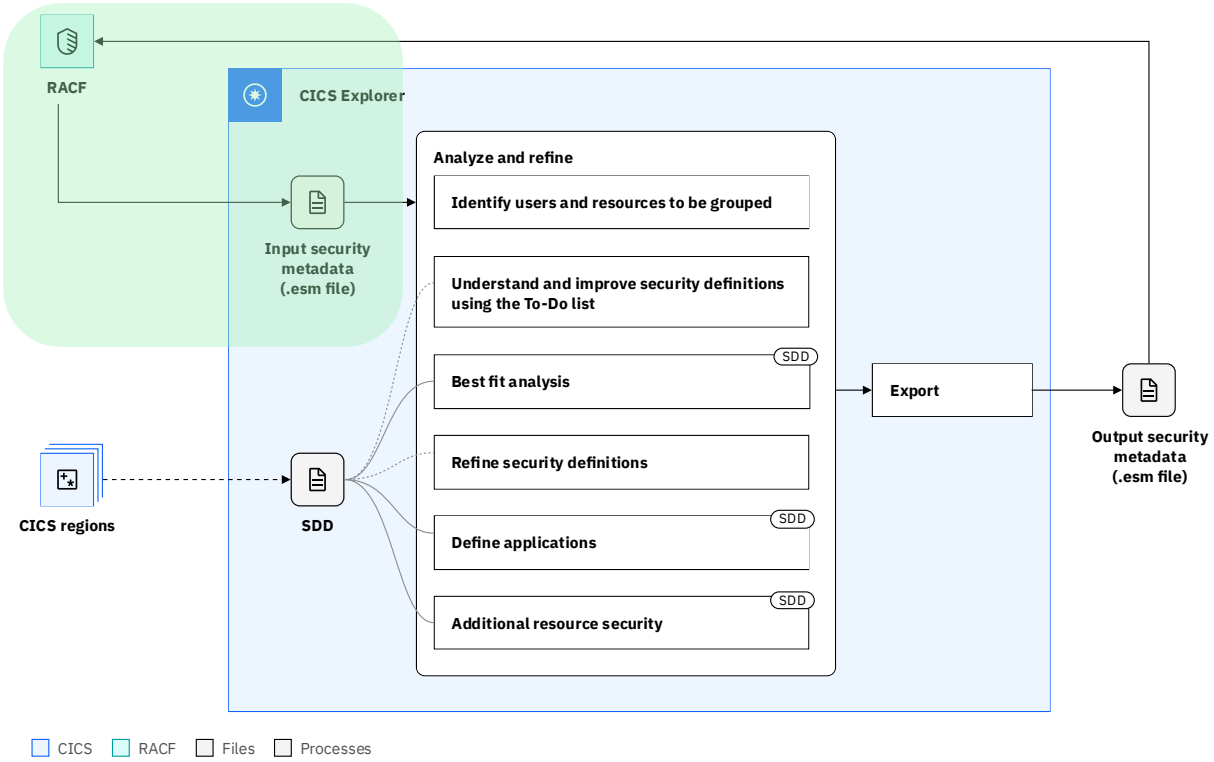
**RACF/ES M Security Definitions**

# Security Discovery Process




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

# Import RACF Definitions




- 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

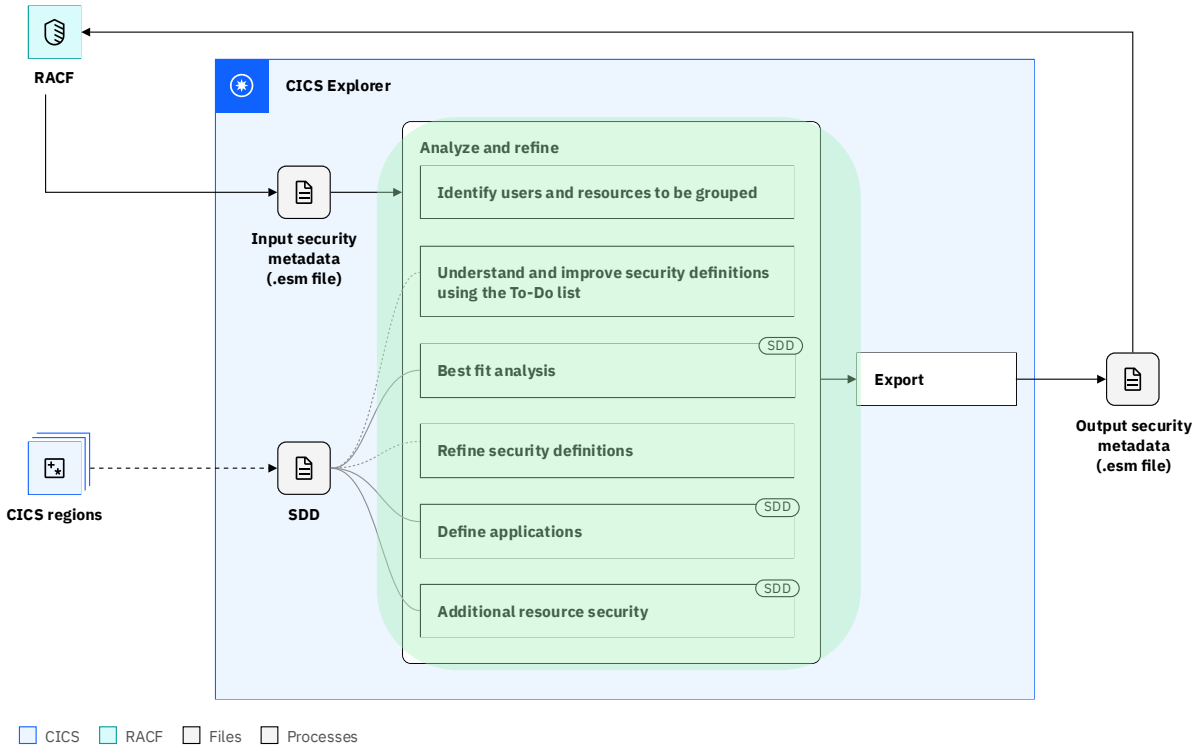
## DFH$R2SM

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

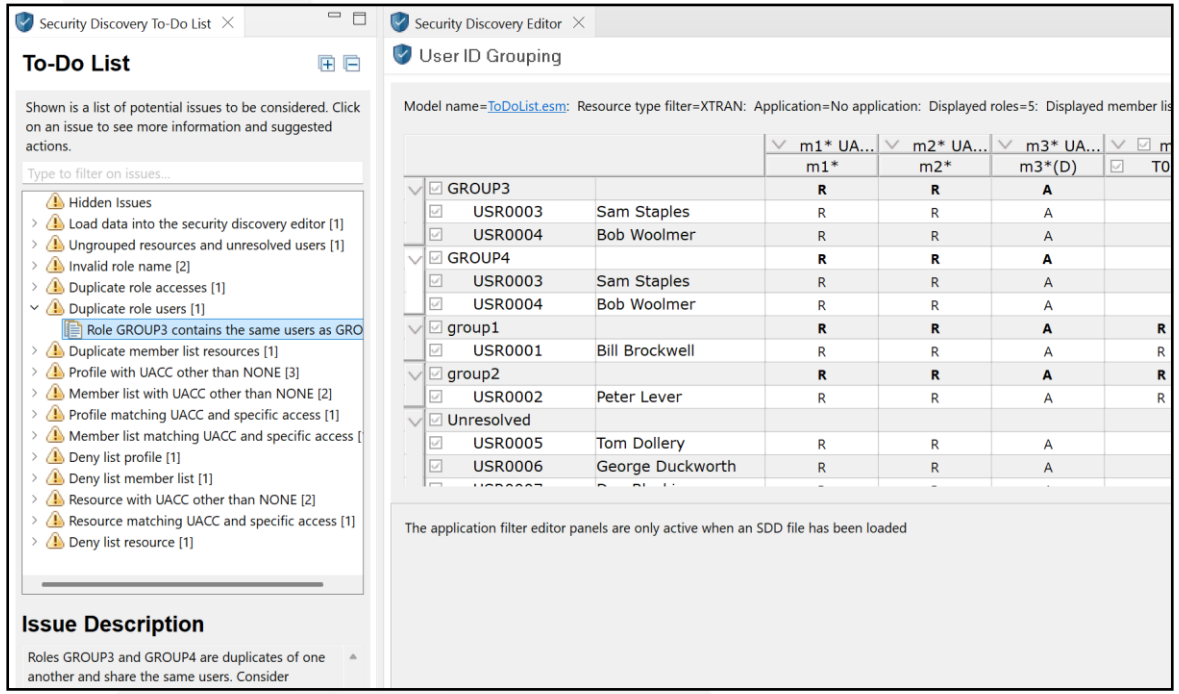
## Security metadata

```
--- # 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
```

# Analyze Security Definitions in CICS Explorer




## CICS Explorer - Security Discovery Perspective

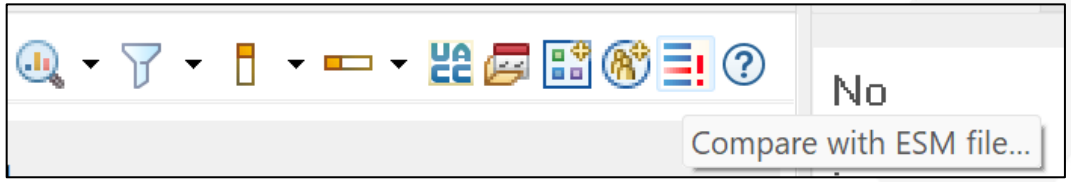



Use security metadata to

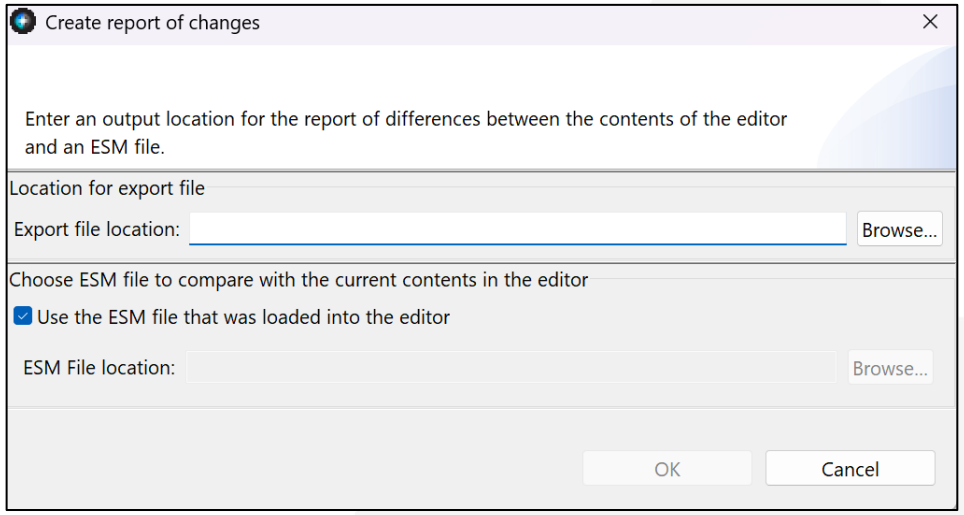
- Identify areas where existing definitions do not match best practice or zero trust objectives
- Improve existing definitions and move to better role-based access controls

# Compare security changes with 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 |

# DEMO 1
# USING THE ESM FILE
# (AVAILABLE AT CICS 6.1)

# Capturing Security Discovery Data

Requires CICS TS 6.2 or later – run in production

When resource is used the following info captured

- User ID
- Transaction
- Origin transaction

Each access captured once only

- Each level of access recorded

Captured in 64-bit memory

Long running process

Small performance overhead

Activated by PLT or CICS Explorer interface

Captures the security access regardless of security settings

- Ignores X*** SIT parms
- Ignores CMDSEC & RESSEC

Data written to a log stream daily

- Also, at shutdown
- On demand

Individual captures different regions merged together offline

# Enabling Discovery

An SPI is provided in CICS TS 6.2

- Enable discovery of all or selected security classes
- Transaction data always collected
- Status of data collection
- How much data collected
- Perform a write of the data

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

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

PERFORM SECDISCOVERY WRITE
```

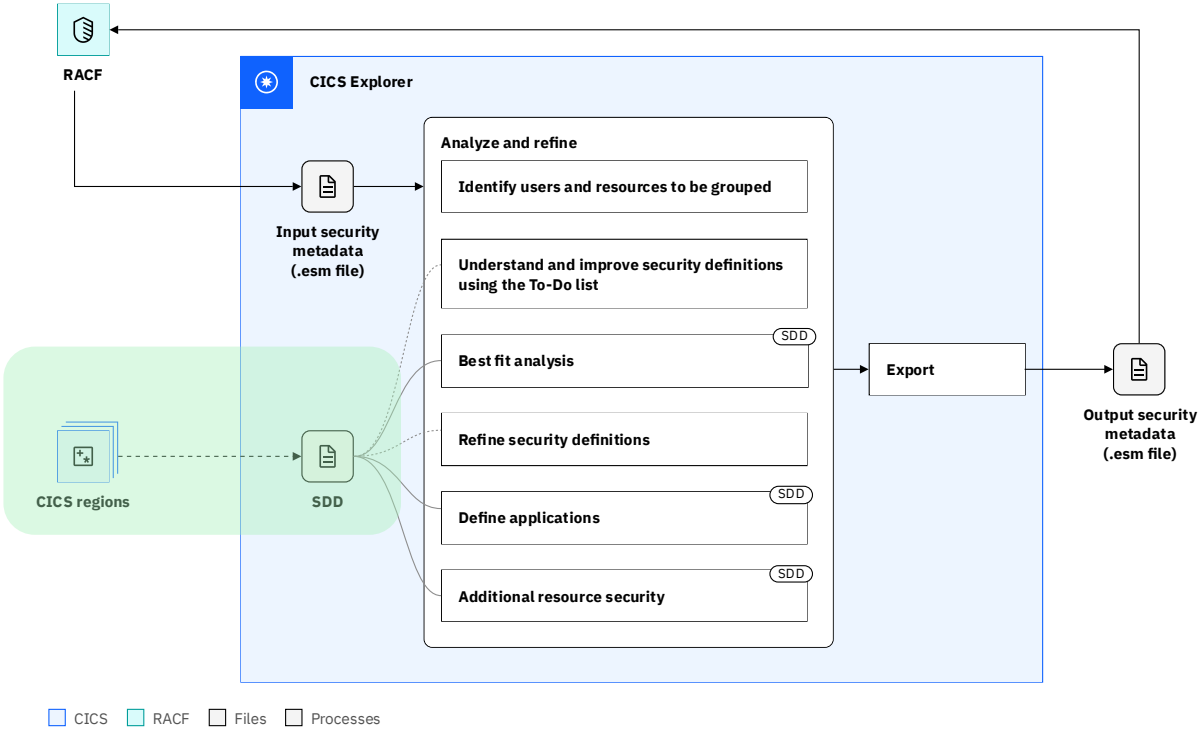
# How much data to collect

Expect the discovery to be enabled for a long period of time

- Capture ‘business as usual’ periods
- Capture special periods of demand
  - Christmas
  - Weekends
  - Black Friday
- Statistics inform number of records captured
- Data collection begins to tail off

```
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




- 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,TCICSTR
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,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
```

# DEMO 2
# USING THE CICS SECURITY DISCOVERY DATA FILE (AVAILABLE AT CICS 6.2+)

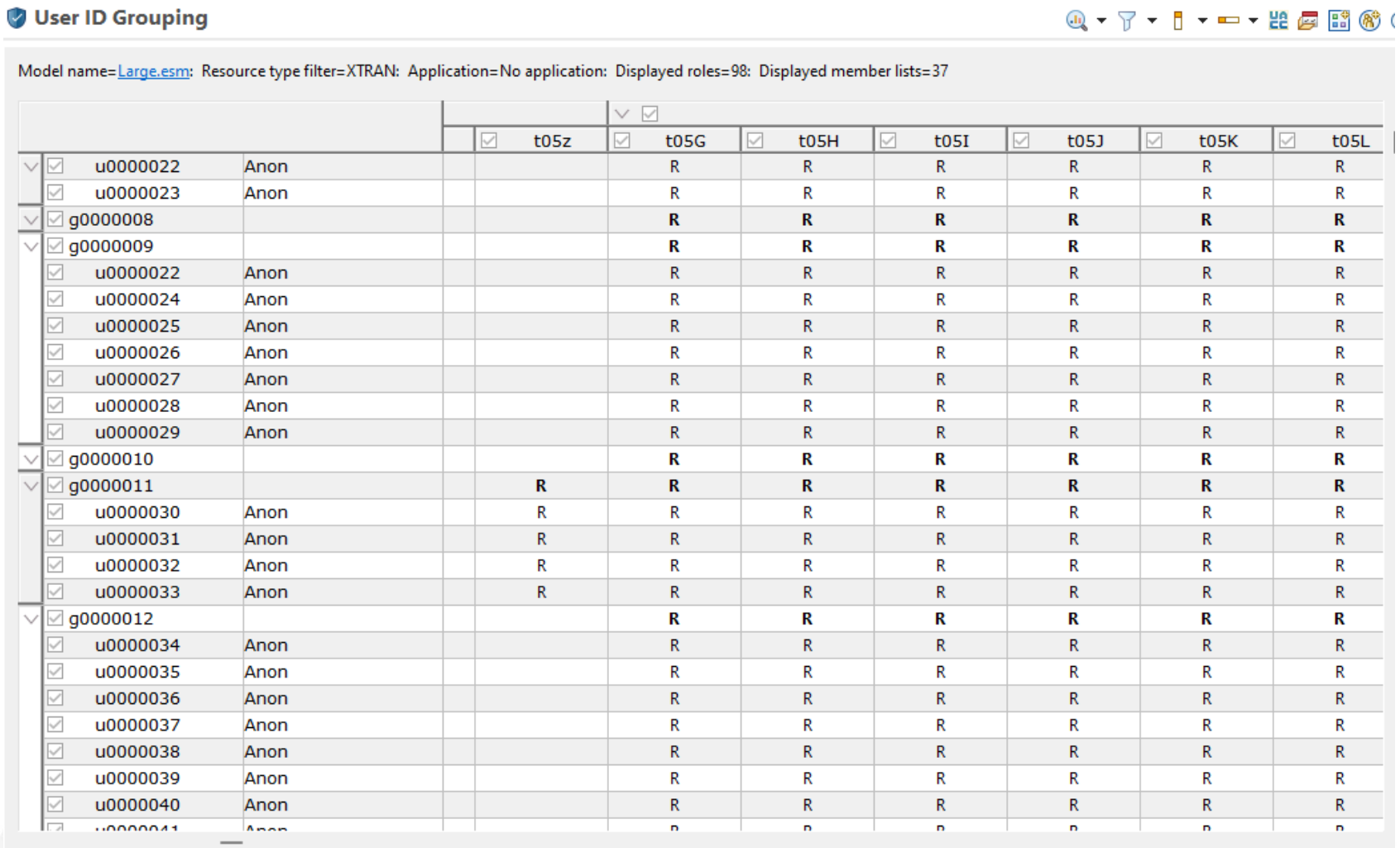
# Summary of demonstrations

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

# Review ESM Data

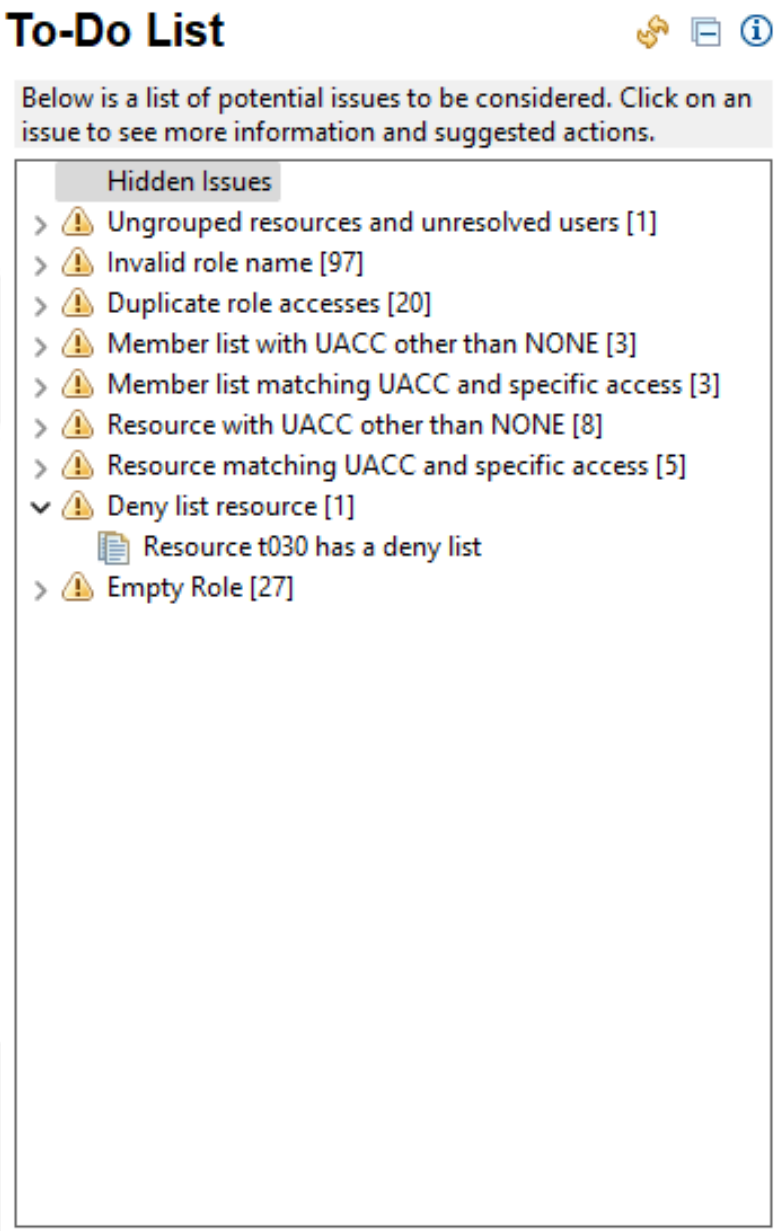


User ID Grouping

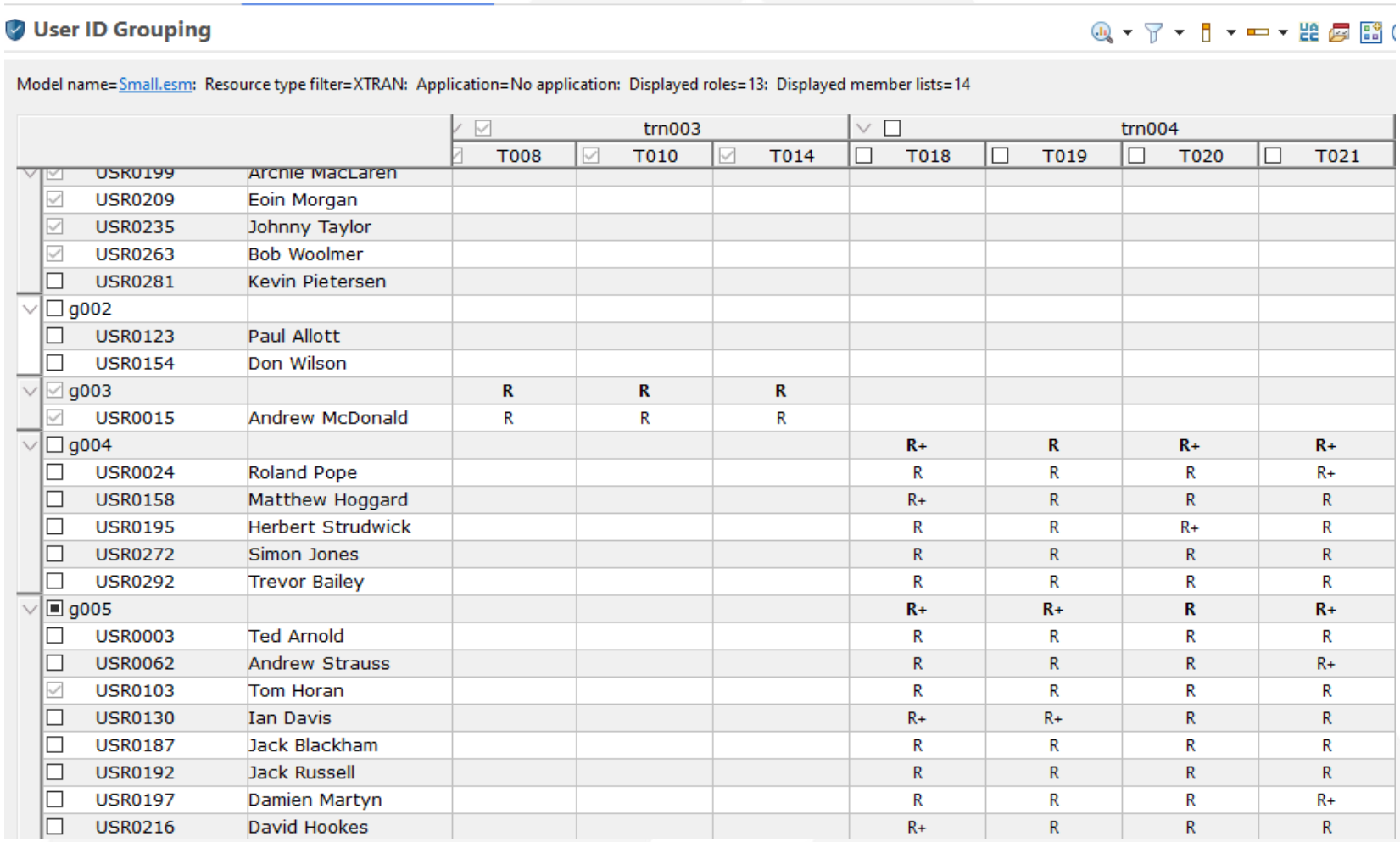
Model name=Large.esm: Resource type filter=XTRAN: Application=No application: Displayed roles=98: Displayed member lists=37

| | | 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 |

# The To-do List



# Analysis Process



**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 |

# Overlaying Discovery Data (SDD)

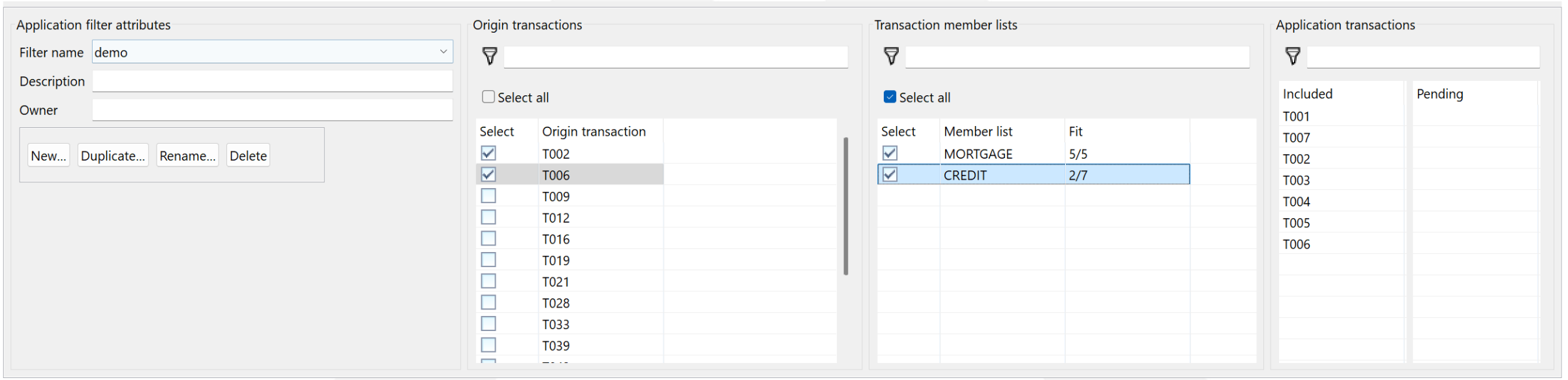
SHARE
EDUCATE • NETWORK • INFLUENCE

**User ID Grouping**

Model name=v12-10u-demo-renamed.esm: Resource type filter=XTRAN: Application=No application: Displayed roles=12: Displayed member lists=12

| | | | CURRENT | | | EOD | IN | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | T019 | T020 | T021 | T026 | T050 | T009 | T011 |
| ☑ | CLERKS | | **Rr** | **Rr** | **Rr** | **Rr** | | | |
| ☑ | USR0024 | Roland Pope | Rr | Rr | R | Rr | | | |
| ☑ | USR0158 | Matthew Hoggard | Rr | R | Rr | Rr | | | |
| ☑ | USR0195 | Herbert Strudwick | Rr | R | Rr | R | | | |
| ☑ | USR0272 | Simon Jones | Rr | Rr | Rr | Rr | | | |
| ☑ | USR0292 | Trevor Bailey | Rr | Rr | Rr | Rr | | | |
| ☑ | HR | | | | | | | **Rr** | **Rr** |
| ☑ | USR0123 | Paul Allott | | | | | | Rr | Rr |
| ☑ | USR0154 | Don Wilson | | | | | | Rr | Rr |
| ☑ | MANAGERS | | | | | | | | |
| ☑ | USR0149 | Dick Tyldesley | | | | | | | |
| ☑ | OPS | | **Rr** | **Rr** | **Rr** | **Rr** | **Rr** | | |
| ☑ | USR0003 | Ted Arnold | Rr | Rr | Rr | R | R | | |
| ☑ | USR0062 | Andrew Strauss | Rr | Rr | R | Rr | R | | |
| ☑ | USR0103 | Tom Horan | Rr | Rr | Rr | R | Rr | | |
| ☑ | USR0130 | Ian Davis | R | R | Rr | R | Rr | | |
| ☑ | USR0187 | Jack Blackham | R | Rr | Rr | R | R | | |
| ☑ | USR0192 | Jack Russell | Rr | Rr | Rr | Rr | R | | |
| ☑ | USR0197 | Damien Martyn | Rr | Rr | R | R | Rr | | |
| ☑ | USR0216 | David Hookes | Rr | Rr | Rr | R | R | | |
| ☑ | USR0238 | Tom Curran | Rr | Rr | Rr | Rr | Rr | | |

# Application Filter



# Create Security Definitions

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 with almost zero 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?

# Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

**Submit a session evaluation** for each session you attend:

www.share.org/evaluation