

# Key Vulnerabilities & How To Protect Against Them

---

**IBM i Security Workshop**



# Presenter



## Alan Hamm

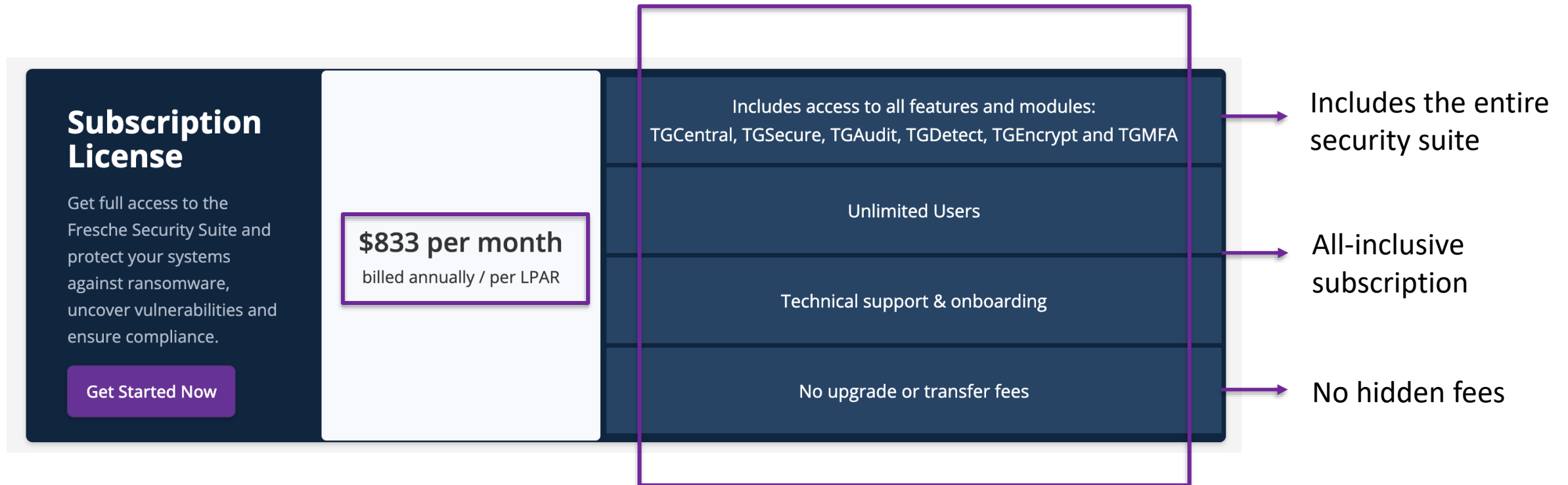
Senior Security Engineer  
alan.hamm@freschesolutions.com

- Over 25 years of experience in the IT industry, specializing in IBM i security.
- Leverages development background to solve automation and configuration problems.
- 17 years as an application developer, systems integrator, business analyst, and data center lead.

# Agenda

- Introduction
- TGSecurity Suite: Overview
- TGSecurity Suite: Subscription Models
- How to Secure:
  - Network Security & Exit Points >> Network Monitoring
  - IFS & Object Authority >> Zero Trust
  - Access Management >> Privileged Access Management
  - SIEM and Forensic Accounting >> Security Event Notifications
  - Auditing and Compliance >> Security Logging/Auditing
- Assessment Report: Sample

# Powerful Security in an Affordable Subscription Model



# Security Services & Flexible Subscriptions

## Custom Licenses

Looking for flexible one-time or unlimited licensing options, Fresche Security is also available via convenient enterprise models. Connect with us to learn more about our custom options.

[Discuss Your Options](#)

## Enterprise Licenses Unlimited Licenses

Flexible Terms

## IBM i Security Services

Partner with experienced IBM i (AS/400, iSeries) security professionals who can help you identify & prioritize vulnerabilities and guide you on improving your security position going forward.

[Security Assessment](#)  
Starting as low as \$0 >

Self assess with free trial

[Security strategy consulting](#)  
Speak with an expert >

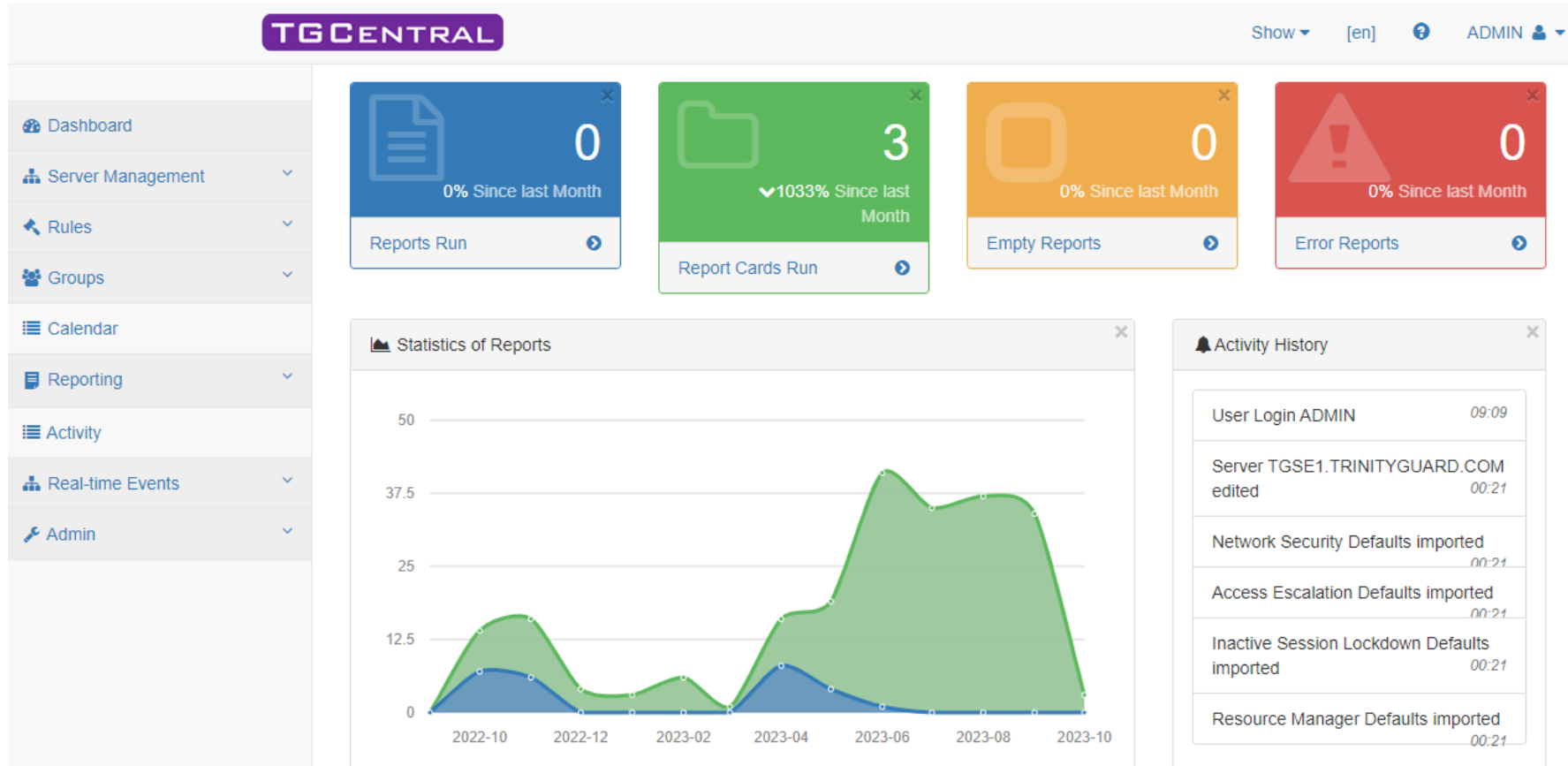
[Security Consulting](#)  
20hr expert services bundle \$5000 >

Affordable access to IBM i security experts

[Penetration Testing](#)  
\$5,750/LPAR >

Trusted advisors Fresche & DXR (Carol Woodbury)

# The GUI Interface



# The GUI Interface

The screenshot displays the TG CENTRAL web interface. The top navigation bar includes the logo, language settings ([en]), a help icon, and the user name ADMIN. A left sidebar contains a menu with items: Dashboard, Server Management, Servers, Server Groups, Rules, Groups, Calendar, Reporting, Activity, Real-time Events, and Admin. The main content area is divided into two sections. The first section, titled 'Servers', features '+ Add' and 'Refresh' buttons, a 'Show 5 entries' dropdown, and a search box. It contains a table with two server entries: TGSE1.TRINITYGUARD.COM (IP: 172.17.172.243, OS: V7R4M0) and TGQE5.TRINITYGUARD.COM (IP: 172.17.172.239, OS: V7R3M0). Below the table are 'First', '1', and 'Last' navigation buttons. The second section, titled 'Activity History at TGSE1.TRINITYGUARD.COM', includes 'Report Activity', 'Activity', 'Schedule', and 'Details' buttons, followed by '+ Run' and 'Refresh' buttons, a 'Show 20 entries' dropdown, and a search box. It contains a table with four report entries for 'PCI DSS 4.0' with dates from 2023-09-30 to 2023-10-03. The first entry shows a progress bar at 66/79.

**Servers**

Server Name	IP Address	OS Version	Platform	Status	Action
TGSE1.TRINITYGUARD.COM	172.17.172.243	V7R4M0	IBM i	Managed	Action
TGQE5.TRINITYGUARD.COM	172.17.172.239	V7R3M0	IBM i	Managed	Action

**Activity History at TGSE1.TRINITYGUARD.COM**

Report Name	Date	Status	Action
PCI DSS 4.0	2023-10-03 04:00	66/79	Action
PCI DSS 4.0	2023-10-02 04:00	Completed	Action
PCI DSS 4.0	2023-10-01 04:00	Completed	Action
PCI DSS 4.0	2023-09-30 04:00	Completed	Action

# The GUI Interface

**TGCENTRAL** [en] ? ADMIN

- Dashboard
- Server Management
  - Servers
  - Server Groups
- Rules
  - Job Activity Monitor
  - Network Security
  - Socket Rules
  - Remote Exit Rules
  - Exit Point Config
  - Defaults
  - Access Escalation Mgmt.
  - Inactive Sess. Lockdown
  - Resource Manager
  - User Profile Manager
  - Detect Monitors
  - Database Encryption
  - Command Security

### Remote Exit Rules

+ Add Refresh

Show 50 entries Search

Server	User/Group	Operation Server	Function	Client IP	Calendar	Alert Status	Exit Rule Action	Object Details	Action
TGSE1.TRINITYGUARD.COM	*PUBLIC	*ALL		*ALL	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	*ALL	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.11.12.35	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.27.81.32	*NONE	*YES	*PASS		Action
*ALL	*PUBLIC	*ALL		*ALL	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	*ALL	10.11.12.*	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.27.81.*	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	:ADMIN	FILE	*ALL	10.*	*NONE	*NO	*PASS	/home/PMB/mydir	Action
TGSE1.TRINITYGUARD.COM	PMB	DBSQL	*ALL	10.*	*NONE	*NO	*PASS	FINANCE/CUSTMAST.FILE	Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	*ALL	10.27.*	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	DBSQL	*ALL	10.27.81.26	*NONE	*YES	*PASS	FINANCE/CUSTMAST.FILE	Action
TGSE1.TRINITYGUARD.COM	:ADMIN	FTPSRV	LOGON	10.11.*	*NONE	*YES	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	:FILEGRP		10.27.81.30	*NONE	*NO	*PASS	/TrinityGuard/Reports	Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.27.81.23	*NONE	*YES	*FAIL		Action

First 1 Last



# The GUI Interface

The screenshot shows the TGCENTRAL web interface. At the top, there is a header with the logo 'TGCENTRAL', a language selector '[en]', a help icon, and a user profile 'ADMIN'. A left sidebar contains a navigation menu with items: Dashboard, Server Management, Servers, Server Groups, Rules, Groups, Calendar, Reporting, Reports, Report Cards, Activity, Real-time Events, and Admin. The main content area is titled 'List of Roles' and includes '+ Add' and 'Refresh' buttons. Below the title, there is a 'Show 50 entries' dropdown and a search box. A table lists the following roles:

Name	Description	Built-in	Functions
Admin	Power user with access to all Functionality	Yes	Action
Auditor	Ability to create, view, run, and rerun reports. Auditor has the ability to view rules (ie JAM), but not change or delete them.	Yes	Action
Creator	Responsible for creating reports, and should also have everything that a Reader has.	Yes	Action
Helpdesk	Usually helps users troubleshoot issues with their reports, or logging in, etc. Hence they can generally do everything an Auditor can do, and actions to users, except delete them.	Yes	Action
Reader	Ability to view reports and delta reports.	Yes	Action
Super User	Everything the Help Desk has, plus the ability to maintain rules and delete users. This would be the equivalent of the Admin, minus Rules, and Settings.	Yes	Action

At the bottom of the table, there is a pagination control showing 'First', '1', and 'Last'.



**Poll: What layers of your IBM i have you secured?**



# TG Security Suite: Overview

- Accessing the Suite
- Authorizing users
- Checking product version and license
- Assessing Exit Point defaults

```
Audit Status . . . . . : *YES
Audit Journal . . . . . : TGJRN
Audit Journal Library . . . . : TGDATA
Audit Configuration Changes. . : Y
Alert Status . . . . . : *YES
Alert Message Queue . . . . . : TGMSGQ
Alert Message Queue Library. . : TGDATA
TELNET AutoSignon Allowed . . : *NO
Primary Group Inheritance. . . : *YES
Supplemental Group Inheritance : *YES
Enable Debug . . . . . : *NO
```

- TGMENU
- 70. Work with TG Product Users or edtautl tgautl
- 80. Licensing Status
- TGSecure->Network Security-> Network Security Defaults
- TGSecure->Network Security-> Exit Point Configuration->F7

```
Network Server . . . . . : *ALL
Exit Point . . . . . : *ALL
Exit Format . . . . . : *ALL
Exit Description . . . . . : All Re
Audit Status . . . . . : *YES
Security Status . . . . . : *NO
Alert Status . . . . . : *ALL
Smart Mode . . . . . : *YES
Collector Status . . . . . : *ALL
```

# Network Security and Exit Points

How to objectives:

Log detailed exit point information

\*\*No exit points by default = No detailed logging/monitoring

To add/remove exit programs:

TGMENU->2. TGSecure->1. Network Security->10. Exit Point Configuration

or

TGNTWCFG

TGNTWCFG SERVER(\*ALL) ACTION(\*ADDCYC) RUNI(\*YES)

OR

TGNTWCFG SERVER(\*FTP) ACTION(\*ADDCYC) RUNI(\*YES)

TGNTWCFG SERVER(\*DATABASE) ACTION(\*ADDCYC) RUNI(\*YES)

TGNTWCFG SERVER(\*FILE) ACTION(\*ADDCYC) RUNI(\*YES)

TGNTWCFG SERVER(\*DDM) ACTION(\*ADDCYC) RUNI(\*YES)

TGNTWCFG SERVER(\*SOCKET) ACTION(\*ADDCYC) RUNI(\*YES)



# Network Security and Exit Points

Best practices – deny by default - modify \*PUBLIC (default rule)

```
User Name . . . . . : *PUBLIC +
Client IP . . . . . : *ALL
Operation Server . . : *ALL +
Calendar . . . . . : *NONE +
Alert Status . . . . : *NO
Action . . . . . : *FAIL
Rule Description . . : Default Public Rule
Type of Object. . . . : *NONE
```

Generate/View FTP transactions:

```
cmd
ftp 172.17.172.240
cd /demo/public
cd /demo/it
cd /demo/hr
```

How to \*PASS transactions:

- Allow individual User - FTPSRV LOGON
- Allow using user group :FTPUSERS - FTPSRV LOGON using
- Allow QTCP \*PRE \*AIPASS - FTPSRV INIT
- Allow QTCP \*PRE \*TRUSTED - FTPSRV INIT

# IFS and Object Authority

Best practices – deny by default - \*PUBLIC \*EXCLUDE

How to secure using QSYS:

Create authority schema APP01\_QSYS

```
Owner = APP01
Authorization list = APP01
*PUBLIC = *AUTL
APP01 = *ALL

*PGM
Owner = APP01
Authorization list = *NONE
*PUBLIC = *USE
APP01 = *ALL
Use adopted authority = *YES
Adopted user profile = *OWNER
```

```
*FILE
Owner = APP01
Authorization list = *NONE
*PUBLIC = *EXCLUDE
APP01 = *ALL

*DTAARAFILE
Owner = APP01
Authorization list = *NONE
*PUBLIC = *EXCLUDE
APP01 = *ALL
```

Object	Type
QSYS/APP01	*USRPRF
QSYS/APP01	*AUTL
QSYS/APP01	*LIB
APP01/FILE01 – FILE04	*FILE
APP01/PGM01 – PGM04	*FILE
APP01/QCLLESRC	*FILE
APP01/QRPGLESRC	*FILE
APP01/VERSION	*DTAARA

# IFS and Object Authority

Zero Trust

Create Object Group :APP01

TGMENU->2. TGSecure->4. Resource Manager->

3. Work with Groups->1. Work with Object Groups->F6

```
Group Name . . . : :APP01
Group Description: APP01
```

Add objects

```
Group Name/Desc.: :APP01    APP01
Subset Criteria - File Sys.: *ALL    Obj.Name: *ALL

2=Edit 4=Delete

Opt  File System  Object  Name
-    *SYS          APP01/*ALL.ALL
-    *SYS          QSYS/APP01.LIB
```



# IFS and Object Authority

Authority schema APP01\_QSYS

TGMENU->2. TGSecure->4. Resource Manager->

1. Authority Schema Configuration->F6

```
Schema ID . . . . . : APP01_QSYS
Schema Description. . . . . : APP01_QSYS
Alert Status. . . . . : *NO
Include IFS or Library Object.: *NO
Filter Details . . . . . : *NONE
Object Scope
Object Name . . . . . : ;APP01
Object Library. . . . . :
Object Type . . . . . :
ASP Name. . . . . : *SYSBAS
Scope Authorities
Object Owner. . . . . : APP01
Authorization List. . . . . : *NONE
Object Primary Group. . . . . : *NONE
Adopt User Profile. . . . . : *USER
Adopt Authority . . . . . : *NO
*PUBLIC Authority . . . . . : *EXCLUDE
```

```
Schema ID . . . . . : APP01_QSYS
Schema Description. . . . . : APP01_QSYS
Alert Status. . . . . : *NO

IFS Scope
IFS Path. . . . . : *NONE

Scope Authorities
Object Owner. . . . . :
Authorization List. . . . . :
Object Primary Group. . . . . :
*PUBLIC Object Authority. :
*PUBLIC Data Authority. . :
```

# IFS and Object Authority

## Define schema

```
Schema ID. . : APP01_QSYS
Description. : APP01_QSYS

2=Edit 3=Copy 4=Delete 5=Display

File Path or      Library  Object  Object  Object  Auth  User  Auth  Exception
Opt Sys  ASP                               Name    Type    Owner  List  Object
_  *SYS *SYSBAS                               :APP01  APP01  *NONE *PUBLIC *EXCLUDE *NO
_  *SYS *SYSBAS                               :APP01  APP01  *NONE APP01  *ALL    *NO
```

```
Schema ID . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : *ALL
Object Library . . . : APP01
Object Type. . . . . : *PGM
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
Adopt User Profile . : *OWNER
Adopt Authority. . . : *YES
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *USE
```

```
Schema ID . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : *ALL
Object Library . . . : APP01
Object Type. . . . . : *PGM
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
Adopt User Profile . : *OWNER
Adopt Authority. . . : *YES
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
```

```
Schema ID . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : APP01
Object Library . . . : QSYS
Object Type. . . . . : *LIB
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : APP01
Object Primary Group.: *NONE
Adopt User Profile . : *USER
Adopt Authority. . . : *NO
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *AUTL
```

```
Schema ID . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : APP01
Object Library . . . : QSYS
Object Type. . . . . : *LIB
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : APP01
Object Primary Group.: *NONE
Adopt User Profile . : *USER
Adopt Authority. . . : *NO
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
```

# IFS and Object Authority

Zero Trust

Run Compliance Report

Take option 22

Or

```
TGAUTCMP SCHID(APP01_QSYS) ARPT(*NO) OUTPUT(*) ENFO(*NO) RUNI(*YES)
```

# IFS and Object Authority

Best practices – deny by default - \*PUBLIC \*EXCLUDE

How to secure using IFS:

Create authority schema APP01\_IFS

Application location = /demo/App01

Owner = APP01

Authorization list = \*NONE

\*PUBLIC = \*EXCLUDE

APP01 = \*ALL

Application support team needs access to logs!

/demo/App01/log

Owner = App01

Authorization list = \*NONE

\*PUBLIC = \*EXCLUDE

APP01 = \*ALL

GRPPGMRS = \*RX



# IFS and Object Authority

## Define schema

```
TGTS1                                     Default Authority Schema - Add
ALAN
Schema ID . . . . . : APP01_IFS          (Name)
Schema Description. . . . . : Application 01 IFS Example
Alert Status. . . . . : *NO              (*YES,*NO)
Include IFS or Library Object.: *IFS      (*SYS,*IFS,*ALL,*NO)  IFS Depth: 99
Filter Details . . . . . : *NONE         (*NONE,Filter Name)  +
Object Scope
Object Name . . . . . : *NONE            (*NONE,*ALL,:TGGRP,Name,Generic*)  +
Object Library. . . . . :                (*ALL,Name,Generic*)
```

```
TGTS1                                     Default Authority Schema - Add
ALAN
Schema ID . . . . . : APP01_IFS          (Name)
Schema Description. . . . . : Application 01 IFS Example
Alert Status. . . . . : *NO              (*YES,*NO)
IFS Scope
IFS Path. . . . . : /demo/app01
Scope Authorities
Object Owner. . . . . : APP01            (*SAME,Name)
Authorization List. . . . . : *NONE      (*NONE,*SAME,Name)
Object Primary Group. . . . . : *NONE    (*NONE,*SAME,Name)
*PUBLIC Object Authority. . . . . : *NONE (*ALL,*NONE,*OBJEXIST,
*PUBLIC Data Authority. . . . . : *EXCLUDE (*NONE,*RWX,*RX,*RW,*M
```

```
TGTS1                                     Aut
ALAN
Schema ID . . . . . : APP01_IFS2
Schema Description . : Application 01 IFS Example
File System. . . . . : *IFS
IFS Scope
IFS Path . . . . . : /demo/app01/log

IFS Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE

User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *NONE
Data Authority . . . : *EXCLUDE
-----Object-----
Mat  Exist  Alter  Ref
```

```
TGTS1                                     Aut
ALAN
Schema ID . . . . . : APP01_IFS2
Schema Description . : Application 01 IFS Example
File System. . . . . : *IFS
IFS Scope
IFS Path . . . . . : /demo/app01/log

IFS Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE

User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
Data Authority . . . : *RWX
-----Object-----
```

```
TGTS1                                     Aut
ALAN
Schema ID . . . . . : APP01_IFS2
Schema Description . : Application 01 IFS Example
File System. . . . . : *IFS
IFS Scope
IFS Path . . . . . : /demo/app01/log

IFS Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE

User Authority Settings
User Name. . . . . : GRPPGMRS
Object Authority . . : *NONE
Data Authority . . . : *RX
-----Object-----
```

# IFS and Object Authority

Zero Trust

Run Compliance Report

Take option 22

Or

```
TGAUTCMP SCHID(APP01_IFS) ARPT(*NO) OUTPUT(*) ENFO(*NO) RUNI(*YES)
```

### Blueprint

Use Case: Restricted User Provisioning without \*SECADM

Allow Development manager (ALANNONSEC) the ability to enable their service account (APP01) when needed.

# Access Management

## Privileged Access Management

### Create Blueprint APP01\_STATUS\_CHANGE

```
TGTS1                               Blueprint - Add (Step 1/6)
ALAN

Blueprint details
Blueprint ID. . . . . : APP01 STATUS CHANGE
Blueprint Description . . . . . : APP01 STATUS CHANGE
Alert Status. . . . . : *NO

User Scope. . . . . : :APP01

Inactivity Overrides
Inactivity until User Profile is disabled (days). . : *DFT
Inactivity until User Profile is deleted (days). . : *DFT
Object owner for objects owned by deleted profiles. : *DFT
```

```
TGTS1                               Bluepri
ALAN                               User Pro

Blueprint ID . . . . . : APP01 STATUS CHANGE
Description. . . . . : APP01 STATUS CHANGE

Set the User Profile Parameter values.

4=Delete 2=Edit

Opt Parameter          Parameter  Parameter
  Description          keyword   Value
- Status              STATUS   *ENABLED
```

# Access Management

## Privileged Access Management

### Create Blueprint APP01\_STATUS\_CHANGE

```
TGTS1                               Blueprint - Add (Step 3/6)
ALAN                               User Profile Object Authority
Blueprint ID. . . : APP01_STATUS_CHANGE      Description. . . : APP01 STATUS CHANGE
Enter the Object Authority settings.

*USRPRF Object
Object Owner . . . . . : *DFT                (*DFT,Name,*USRPRF)
Owner Authority . . . . . :                   (*CHANGE,*USE,*EXCLUDE,*ALL)
*PUBLIC Authority . . . . . :                   (*AUTL,*USE,*CHANGE,*ALL,*EXCL

*MSGQ Object
Object Owner . . . . . : *DFT                (*DFT,Name,*USRPRF)
Owner Authority . . . . . :                   (*CHANGE,*USE,*EXCLUDE,*ALL)
*PUBLIC Authority . . . . . :                   (*AUTL,*USE,*CHANGE,*ALL)
```

```
TGTS1                               Blueprint - Add (Step 4/6)
ALAN                               Authority List Settings
Blueprint ID . . . . . : APP01_STATUS_CHANGE
Description. . . . . : APP01 STATUS CHANGE
Set the Authority Lists.

4=Delete

Authority Authority
Opt List Value Description
```

```
TGTS1                               Blueprint - Add (Step 5/6)
ALAN                               3rd party Integration
Blueprint ID . . . . . : APP01_STATUS_CHANGE
Description. . . . . : APP01 STATUS CHANGE
Set 3rd Party script to run and Pass User Profile($USRPRF) and/or Description ($TEXT)

4=Delete

Script Script
Opt Type Statement
```

```
TGTS1                               Blueprint - Add (Step 6/6)
ALAN                               Blueprint Permissions
Blueprint ID. . . : APP01_STATUS_CHANGE      Description. . . : APP01 STATUS CHANGE
Authorize admin/help desk users to use the blueprints.

User/Group. . . . . : ALANNONSEC (:TGUSGRP) +
Create Permissions. . . : *NO                (*YES,*NO)
Change Permissions. . . : *YES                (*YES,*NO)
```



Blueprint APP01\_STATUS\_CHANGE

```
ADDAUTLE AUTL(TGAUTL) USER(ALANNONSEC) AUT(*USE)
```

Check it out, test it!

```
TGPRFCMP COMPN(APP01_STATUS_CHANGE) OUTPUT(*) ENFO(*NO) RUNI(*YES)
```

```
TGPRFCMP COMPN(APP01_STATUS_CHANGE) OUTPUT(*) ENFO(*YES) RUNI(*YES)
```

Detect

SIEM and Forensic Accounting

QHST : QSECOFR logins

TGMENU -> 3. TGDetect -> 1. Work with Monitors -> QHST 10 -> 20

### \*NOTE

Not logged/audited by default

### System Values

TGMENU -> 2. TGSecure -> 7. System Value Management -> 1. Work with System Values

### Profile management:

TGMENU -> 2. TGSecure -> 5. User Profile Management -> 5. Profile Inactivity Settings

### Reporting: 😊

TGMENU -> 1. TGAudit

30. Work with Reports (TGWRKRPT)

31. Work with Report Cards (TGWRKCARD)

# Assessment Report

Date:11/03/22  
Time:07:11:00  
System:TGTS1

Category	Description	Number of Violations	Pass/Fail Status	Report Link
Network	Sockets-related exit points not secured	2	FAIL	<a href="#">Detailed Report</a>
Network	Remote server exit points not secured	15	FAIL	<a href="#">Detailed Report</a>
Profiles	System Service Tools users	2	FAIL	<a href="#">Detailed Report</a>
Resources	Integrated File System security	1	FAIL	<a href="#">Detailed Report</a>
Resources	Allow object restore option	1	FAIL	<a href="#">Detailed Report</a>
Resources	Allow user domain objects in libraries	1	FAIL	<a href="#">Detailed Report</a>
Configuration	Auditing control contains AUDLVL and OBJAUD	0	PASS	<a href="#">Detailed Report</a>
Configuration	Attention events are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	Authorization failures are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	All object creations are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	All deletions of external objects on the system are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	Actions that affect a job are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	Networking and communications functions are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	Generic object tasks are audited	0	PASS	<a href="#">Detailed Report</a>
Configuration	OfficeVision are audited	0	PASS	<a href="#">Detailed Report</a>



# Next Steps...

- ✓ Download a Free Trial
- ✓ Subscribe to TGSecurity Suite
- ✓ Speak with a security expert
- ✓ Conduct a Pen Test

## Questions?

[alan.hamm@freschesolutions.com](mailto:alan.hamm@freschesolutions.com)

[info@freschesolutions.com](mailto:info@freschesolutions.com)