Americas' SAP Users' Group

Solution Manager 7.2 SOS:

Mark Hansraj & Jack Mays, IBM

Session ID # 82923

About the Speakers

Mark Hansraj

- SAP Solution manager specialist, IBM
- 15 years of Work with SAP Solution Manager
- I help our Boys scout to make great life choices.

Jack Mays

- SAP Security specialist, IBM
- 16 years of working in SAP security. (Thanks to Kimberly F. Who steered me SOS)
- I build Escape Rooms!

Key Outcomes/Objectives

Utilizing a tool you already have at no additional license cost

Safer systems

Less Risk

Agenda

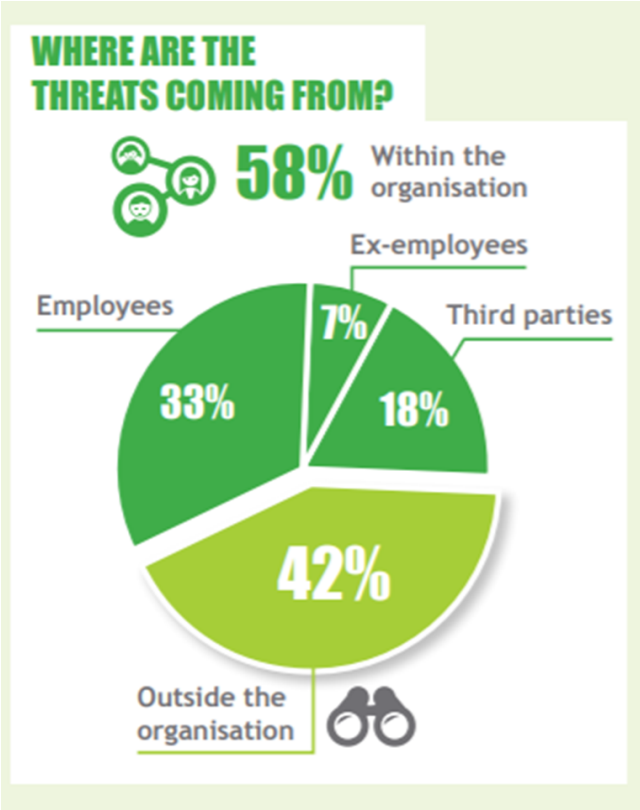
- What is Solution Manager 7.2 SOS?
- Why do I care?
- It really does that?
- General information from the report
- Suggestions

(SOS) or Security Optimization Service Analysis

- This is a wonderful tool that is included in Solution Manager so you already own it. Use it to check your entire system for vulnerabilities both inside and outside of your company.

Business case SAP Security

- **What are the threats?**
- Hackers (Internal and external)
  - Insiders can steal or leak information they can usually do so with far greater ease than outsiders with out evidence of intrusion
  - Employees may unintentionally compromise security, usually caught up in a business requirement
- Market competitors
- Employees



Security Optimization Service Analysis

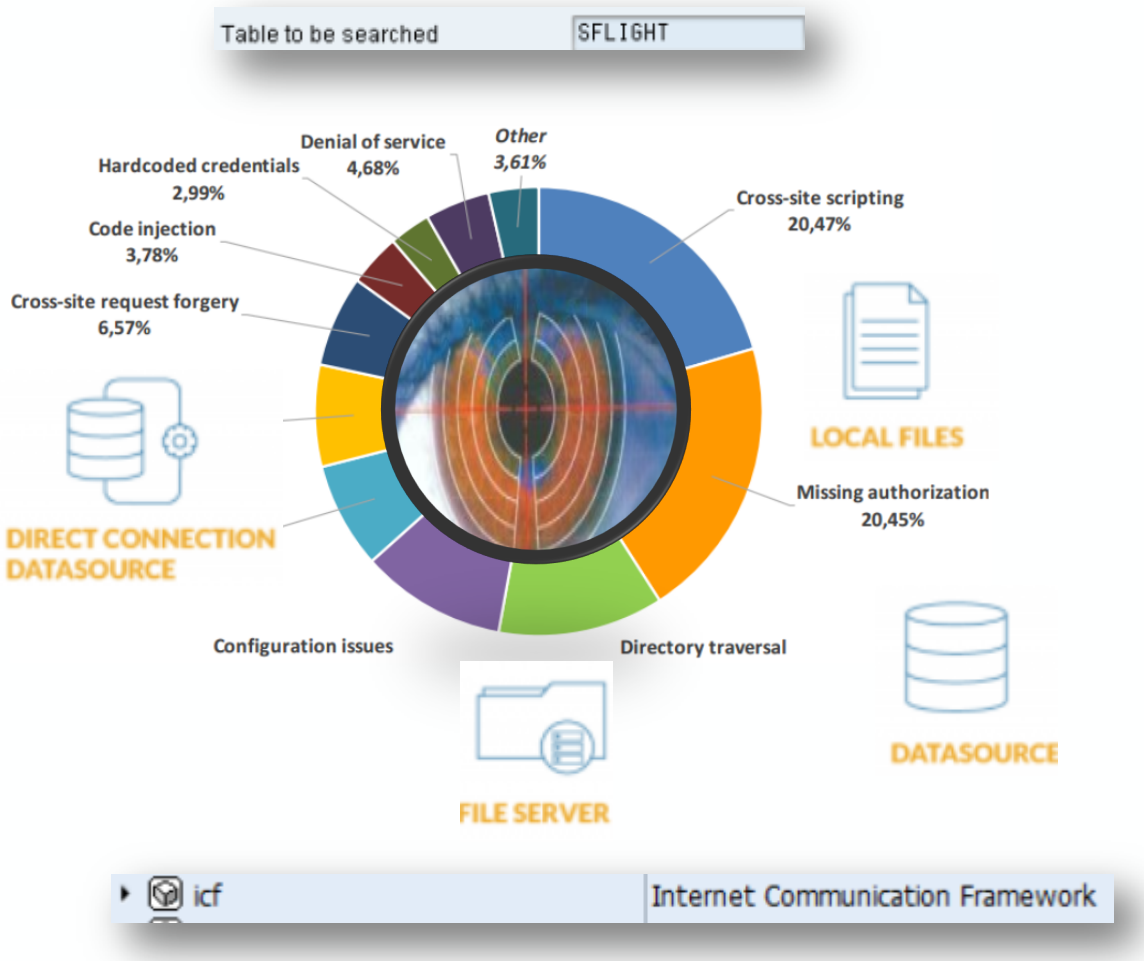
Proactively identifying security risk

Reduce security audits

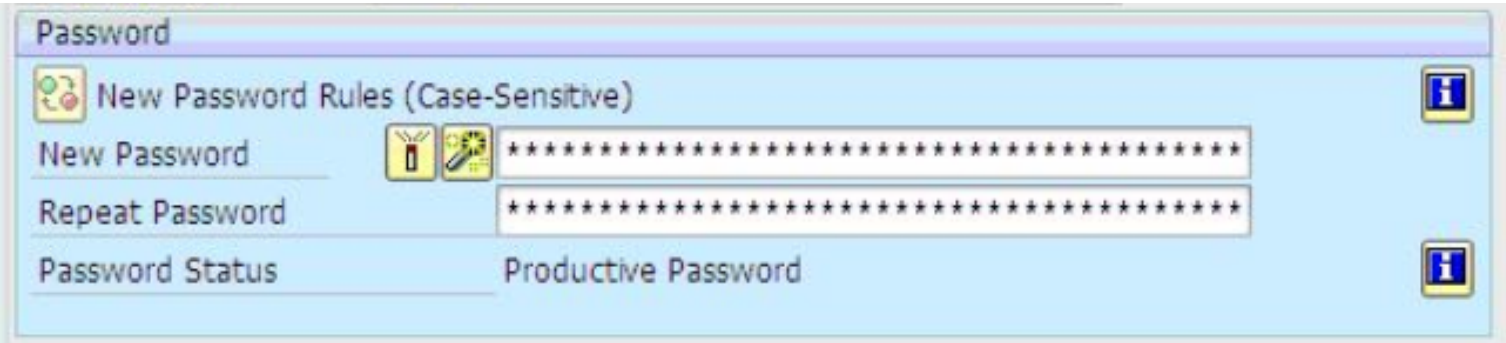
System venerability

We found over 100 ways to hack the system in our report

- Password Policy
- General Authentication
- Administration and authorization
- Data & Program Access
- Change Control
- Development
- Transport Control
- User management
- Super Users
- Role & Authorization Management
- Authorizations
- Internet Communication Framework
- PSE Management



Password Policy

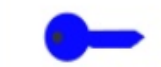


- Complexity
- Initial password
- Security Attacks indicated by user lock due to incorrect Logon Attempts

General Authentication

- Users have not login for extended period of time.
- Security Critical events for end users are not logged in the security Audit log.
- Multiple Logons using same use ID not prevented.
- User account has the right to change password
- Interval for long productive password is too long. *(can continue to try to login as many times as they want)*
- Users have access to Trusted SSO table. *(add system as trusted)*

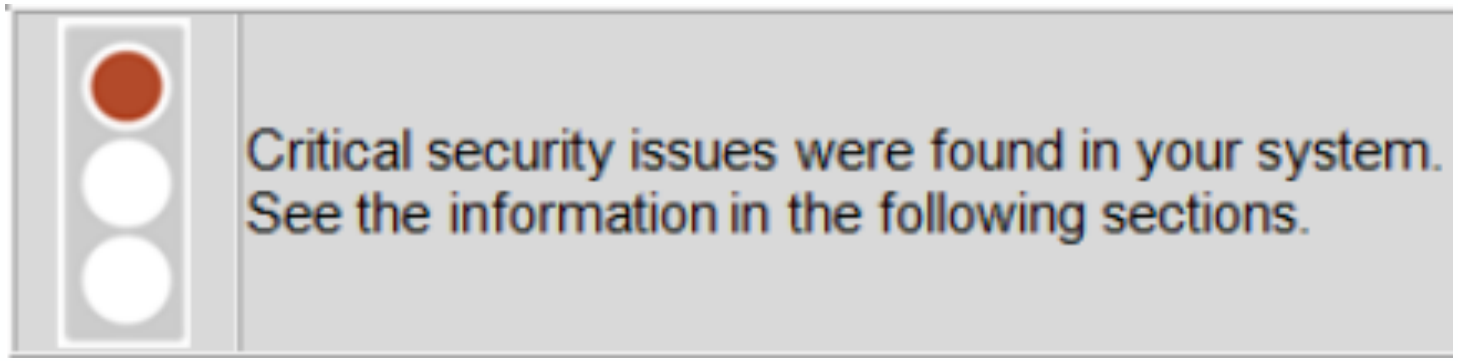
Administration and authorization



- Users other than system Administer can
- maintain system profiles
- start stop application servers
- Authorized to Start/Stop Work processes
- Are Authorized to Lock/Unlock Transactions
- Are Authorized to Maintain Other User's Lock Entries
- Are Authorized to Maintain Own Lock Entries (Inconsistencies due to incorrect deletion of locks are possible)
- Are Authorized to Delete or Reprocess Broken Updates
- Are Authorized to Activate a Trace
- Locks may stay in the database after users terminate their sessions incorrectly.
- Security Audit Log is not active
- Sending Trace Data to Remote Client
- Authorized to Display Other Users Spool Requests (allows unauthorized access to sensitive data)
- Authorized to Change the Owner of Spool Requests(authorization allows unauthorized access to sensitive data contained in spool requests after the ownership has been changed.)
- Are Authorized to Redirect a Print Request to Another Printer
- Are Authorized to Export a Print Request (unauthorized access to sensitive data)
- Are Authorized to Schedule Jobs (Unauthorized background administration can result in: - Inconsistencies - Loss of information - Unauthorized execution of critical programs)
- Are Authorized to Schedule Jobs in External Commands
- Are Authorized to Schedule Jobs Under Another User Id
- Are Authorized to Define External OS Commands
- Are Authorized to Execute External OS Commands
- Are Authorized to View Content of OS Files with AL11
- (Unauthorized access to sensitive data stored in files at operating system level, for example /etc/passwd on UNIX and interface files with sensitive data.)
- Unexpected RFC Connections with Complete Logon Data Found (a direct logon to the target system without any further password check could be possible.)
- Are Authorized to Administer RFC Connections
- Are Authorized to Maintain Trusting Systems
- Permit-all simulation mode is active for the RFC gateway (ignores any existing access control entries)
- Users Are Authorized to Run Any RFC Function without authorization check (In Release 4.6C, for example, there are approximately 14000 RFC-enabled function modules)
- are Authorized to Visualize All Tables via RFC (Unauthorized access to sensitive data by means of RFC)
- Incoming RFC with Expired Password is Allowed
- Users authorized for Trusted RFC
- Users authorized for Trusted RFC which can be called from any calling user
- Unexpected Trusted System Connections Found
- Authorized to Maintain Trusted Systems
- Allowed to Maintain the ALE Distribution Model
- Allowed to Maintain the Partner Profile

Data & Program Access

- Are Authorized to Start All Reports
- Authorized to Display All Tables (Unauthorized access to sensitive data)
- Authorized to Maintain All Tables (Unauthorized maintenance of sensitive data)
- Authorized to Change the Authorization Group of Table
- Authorized to Administer Queries
- Authorized to Execute All Function Modules



Change Control

System Change Option Not Appropriately Configured in the Production System (Threats that arise with the possibility of development in production systems: - Malfunction of system due to programs that have not been tested properly - Unauthorized data access with modified or self-developed programs)

Are Authorized to Change the System Change Option

Are Authorized to Change the Client Change Option(Development is possible in the production system by all of the following persons)

Are Authorized to Create New Clients (logons are permitted with the hard-coded user SAP*)

Users Are Authorized to Delete Clients

Authorized to Development in the Production System

Authorized to Debug and Replace Field Values in the Production System (Unauthorized access to data and functions, since any authorization checks can be bypassed with this authorization)

Authorized to Perform Customizing in the Production System

Authorized to Develop Queries in the Production System

Authorized to Execute CATTs in the Production System (Unauthorized data transfer into the SAP system)

Authorized to Execute eCATTs in the Production System (Unauthorized data transfer into the SAP system)

SAPgui User Scripting Is Enabled (possibility of misuse as it is possible to record sensitive data, for example when creating a new user or changing a user's password.)

Table Logging Is Not Enabled for Import (Lack of information for tracking unauthorized changes to Customizing)

Development

- Development Sources Are Not Scanned for Critical Statements (Coding might contain certain statements (listed as "Critical Statements" in the Code Inspector results) that are critical to security or endanger program stability. Examples include: - INSERT REPORT (ABAP command) - EDITOR-CALL FOR REPORT (ABAP command) - DELETE_USER_ON_DB (function module) - BAPI_USER_* (function modules))

Transport Control

- Are Authorized to Change the TMS Configuration(Inconsistencies due to incorrectly configured CTS)
- Authorized to Start Imports to Production
- Are Authorized to Create and Release Transports
- Authorized to Approve Transports
- Transports Are Not Scanned for Virus

User Management

- Authorized to Maintain Users
- Authorized to Change Their Own User Master Record
- User Master Data Is Not Regularly Synchronized with a Corporate LDAP Directory
- Users with Authorizations for User and Role/Profile/Authorization Maintenance(User and role maintenance must be segregated so that user administrators cannot change their own authorizations.)
- Reference Users Are Used
- Are Authorized to Access Tables with User Data(Avoid dictionary attacks on passwords stored in table USR02)
- Are Authorized to Call Function Modules for User Admin

Super Users

- Unexpected Users Are Authorized to Change a Super User Accounts
- Not all profiles are removed from user SAP*
- User SAP*'s activities are not logged in the Security Audit Log
- User DDIC's activities are not logged in the Security Audit Log
- User EARLYWATCH's activities are not logged in the Security Audit Log

Role & Authorization Management

- Users Are Authorized to Maintain Roles Directly in the Production System
- Users Are Authorized to Maintain Profiles Directly in the Production System
- Users Are Authorized to Maintain Authorizations Directly in the Production System
- SAP Standard Roles Are Assigned to Users
- Profiles on Long Time Locked Users

Authorizations

- Users Are Authorized to Disable Authorization Checks Within Transactions
- Users Are Authorized to Delete an Authorization Check Before Transaction Start
- Global Disabling of Authority Checks Is Not Prevented

Internet Communication Framework

- Are Authorized to Activate ICF Services
- Are Authorized to Administrate the ICM
- Are Authorized to Display the http Server Cache
- Are Authorized to Configure the ICM Monitor(Unauthorized change of ICM services)
- ICM (Internet Communication Manager) Is Active (Backdoor entry to the system via the Web Application Server)

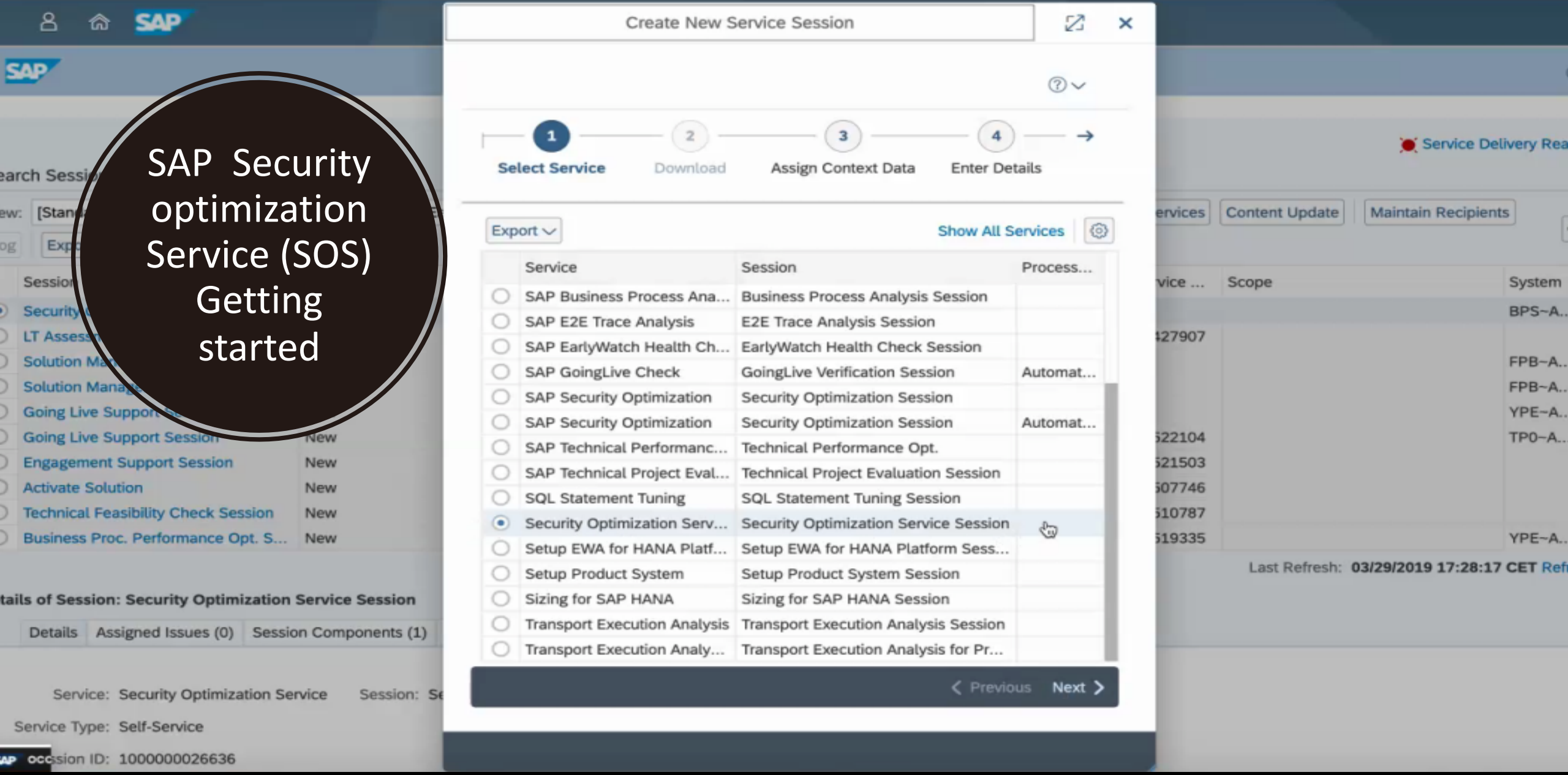
PSE Management

Are Authorized to Maintain the System PSE's

J2EE Engines Allowed to Access the Application Server

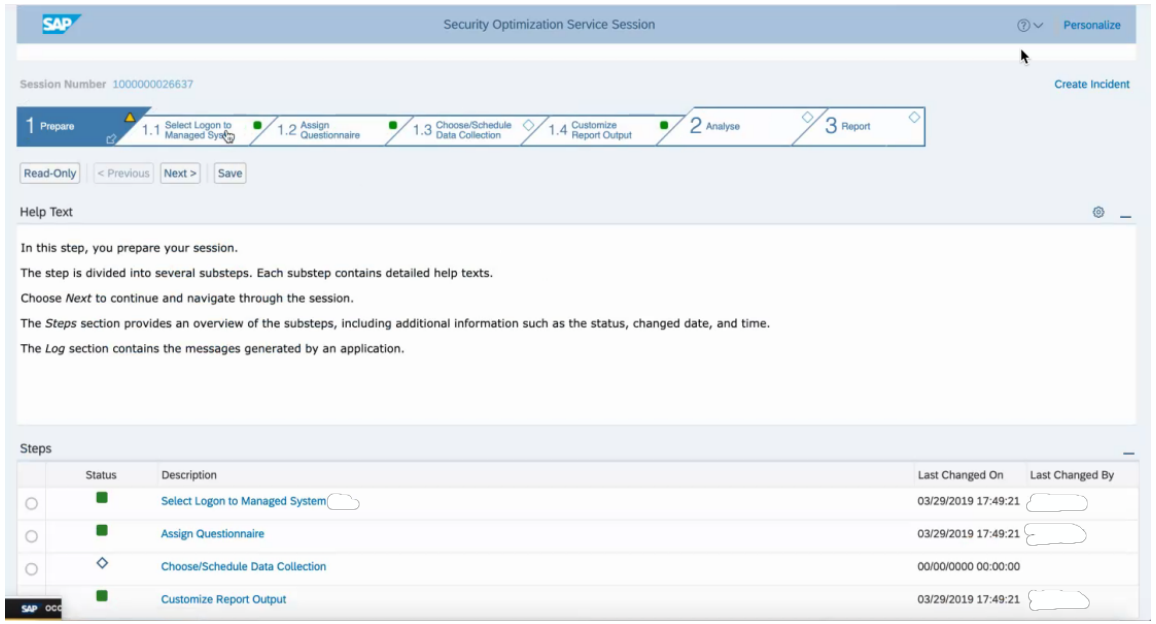
Users Authorized to Maintain the Sending Systems for User Replication

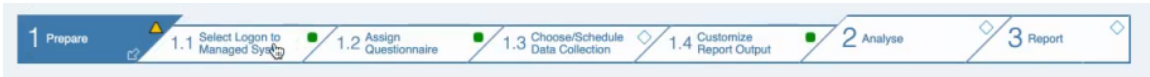
SAP Security optimization Service (SOS) Getting started



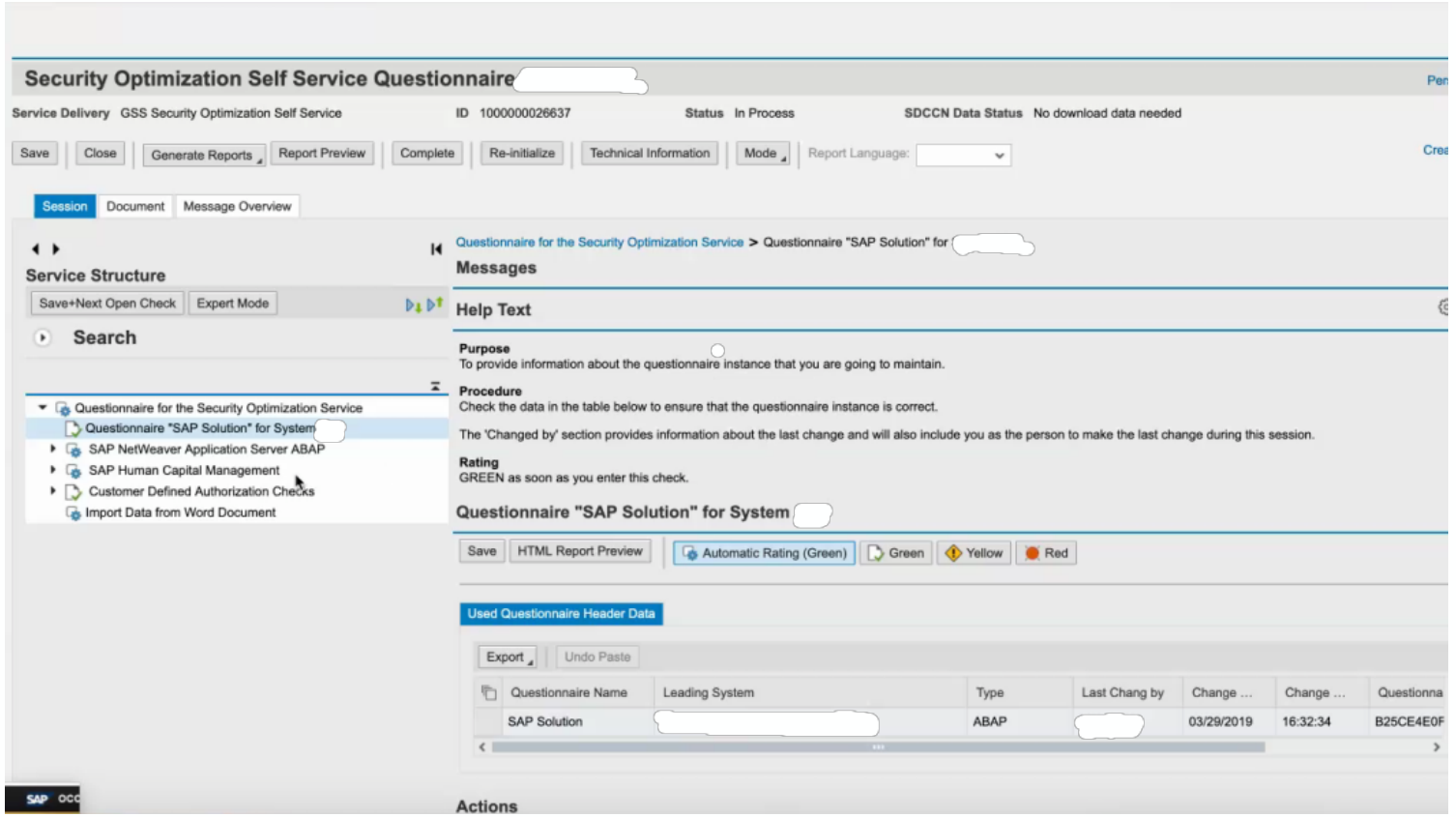
ASUG

Setup

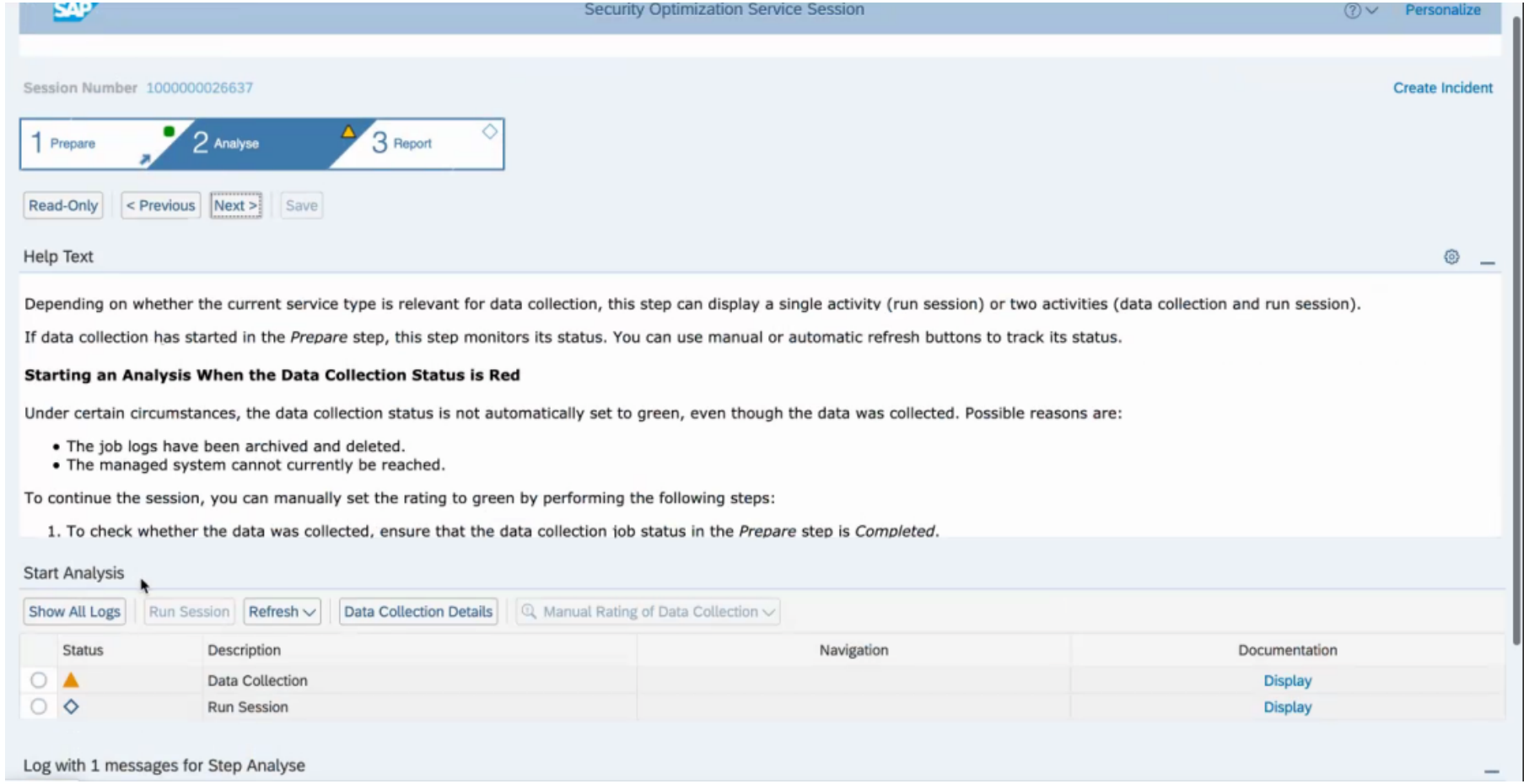

Security Optimization Service Session
Personalize
Session Number 1000000026637
Create Incident
1 Prepare
1.1 Select Logon to Managed System
1.2 Assign Questionnaire
1.3 Choose/Schedule Data Collection
1.4 Customize Report Output
2 Analyse
3 Report
Read-Only
< Previous
Next >
Save
Help Text
In this step, you prepare your session.
The step is divided into several substeps. Each substep contains detailed help texts.
Choose Next to continue and navigate through the session.
The Steps section provides an overview of the substeps, including additional information such as the status, changed date, and time.
The Log section contains the messages generated by an application.
Steps
Status
Description
Last Changed On
Last Changed By
Select Logon to Managed System
03/29/2019 17:49:21
Assign Questionnaire
03/29/2019 17:49:21
Choose/Schedule Data Collection
00/00/0000 00:00:00
Customize Report Output
03/29/2019 17:49:21


1 Prepare
1.1 Select Logon to Managed System
1.2 Assign Questionnaire
1.3 Choose/Schedule Data Collection
1.4 Customize Report Output
2 Analyse
3 Report

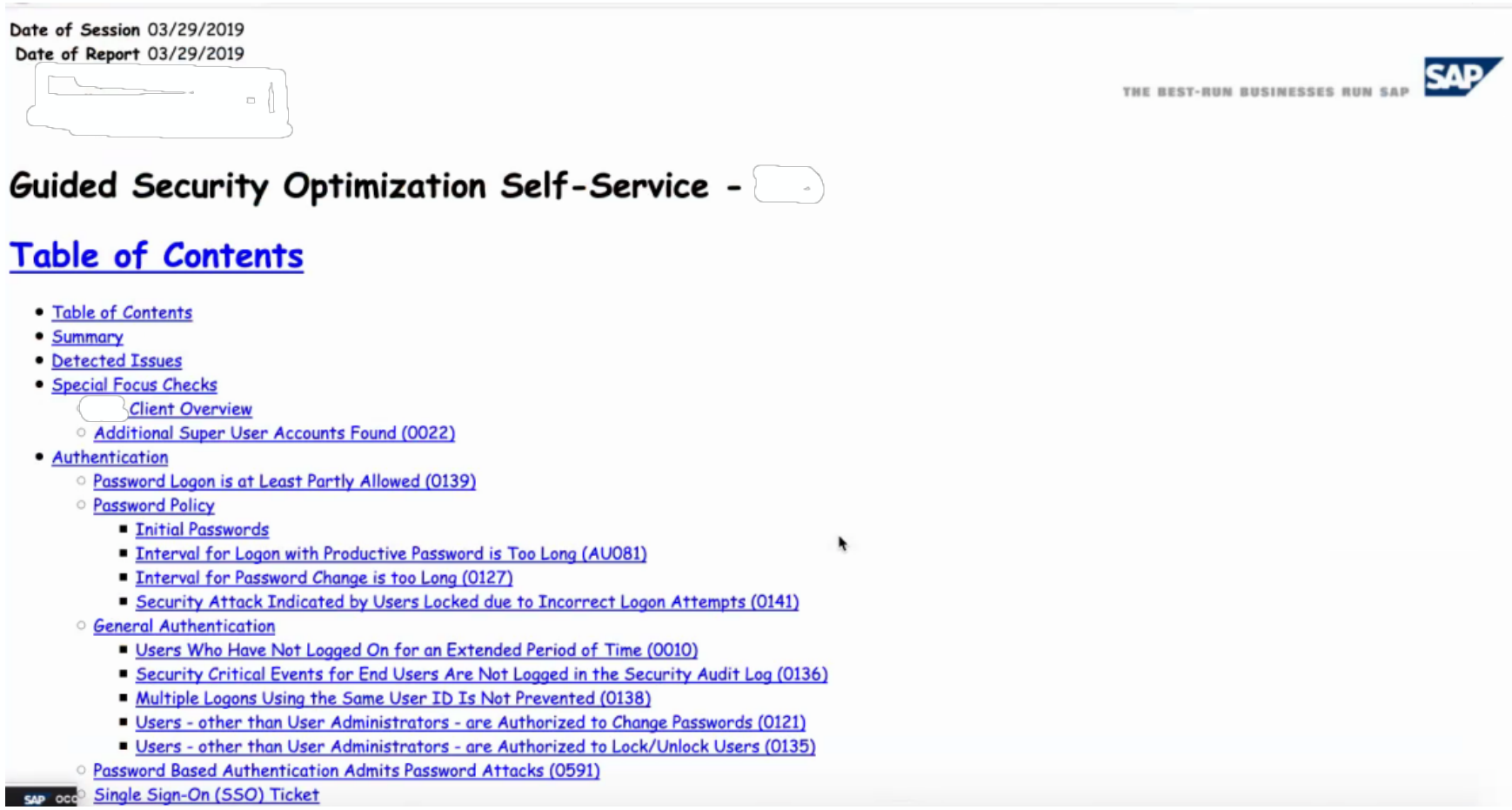
A look at the Questionnaire.



Almost there



What does the report look like?



Date of Session 03/29/2019
Date of Report 03/29/2019

THE BEST-RUN BUSINESSES RUN SAP

Guided Security Optimization Self-Service -

Table of Contents

Report view Example:

- Initial Passwords

Users with Initial Passwords Who Have Never Logged On

Client	Initial Passwords [%]

Evaluated Risk - High

Recommendation:

Check why so many users have initial passwords. Ask these users to change their passwords using the profile parameter login/password_change_for_SSO, for example. Or delete these users if they do not need access to the SAP system.

You can use report RSUSR200 of the User Information System (transaction SUIM) to identity users with initial passwords

Summary

01

Decrease the risk of a system intrusion

02

Ensure the confidentiality of your business data

03

Ensure the authenticity of your users

04

Substantially reduce the risk of costly downtime due to wrong user interaction.

Additional links

- SAP Note 863362 - EarlyWatch Alert (EWA) report - Security chapter
- Change Diagnostics
- Configuration Validation
- Security Audit Log
- SIS264 Securing Remote Access within SAP NetWeaver AS ABAP
- Protecting SAP Applications Against Common Attacks
- Secure Configuration SAP NetWeaver Application Server ABAP
- SAP Security Recommendations: Securing Remote Function Calls (RFC)
- Governance, Risk, and Compliance — Access Control
- Governance, Risk, and Compliance — Process Control
- SAP NetWeaver Identity Management

Take the Session Survey.

- We want to hear from you!

Be sure to complete the session evaluation on the SAPPHIRE NOW and ASUG Annual Conference mobile app.

ASUG

Presentation Materials

Access the slides from 2019 ASUG Annual Conference here:

http://info.asug.com/2019-ac-slides

Q&A

For questions after this session, contact us at MH1@IBM.COM and Jack.Mays1@IBM.COM.

Let’s Be Social.

Stay connected. Share your SAP experiences anytime, anywhere.

Join the ASUG conversation on social media: **@ASUG365 #ASUG**

ASUG