

How to **minimize the attack surface** of hybrid SAP landscapes?

Dr. Hendrik Mueller, SAP SE

Public



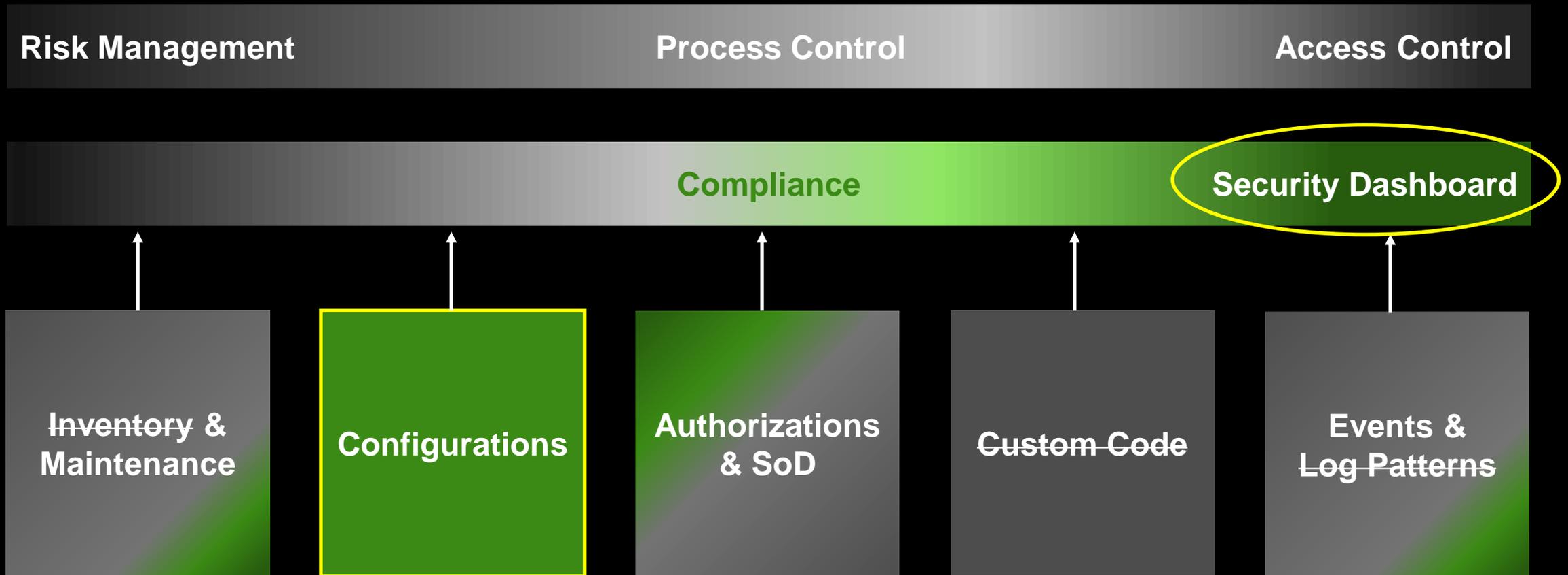
Agenda

1. Warm-up
2. Adoption Journey (SAP & Custom Baseline – Security Notes – Authorizations, RFC, ...)
3. Adoption Journey (Integration with Alerting and Reporting processes)
4. Questions & Discussion

Goal: Automated Security Monitoring & Dashboard for static security checks



Security & Compliance – Aspects addressed by SAP Focused Run

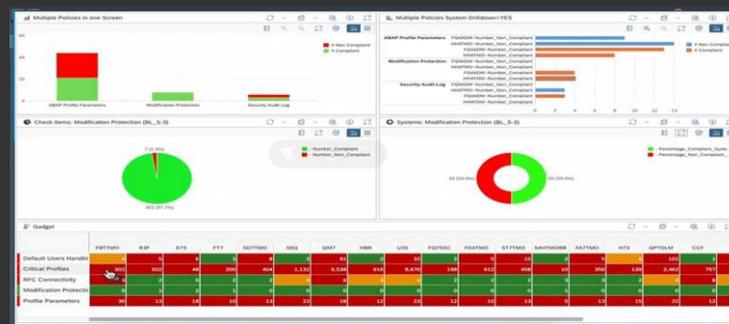
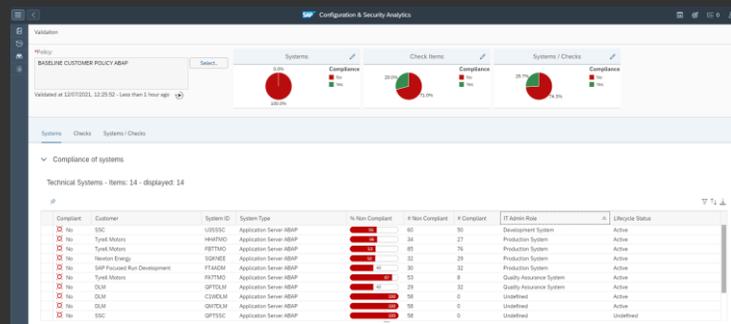


SAP Focused Run for Configuration & Security Analysis



- Enable **central governance** of software levels and configuration settings
- Integrate Security and Compliance into **automated Operation Processes**
- Support **flexible evolution** of a comprehensive configuration and security monitoring

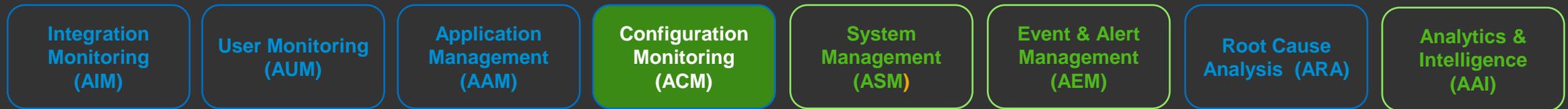
Configuration and Security Analysis



SAP Analytics Cloud

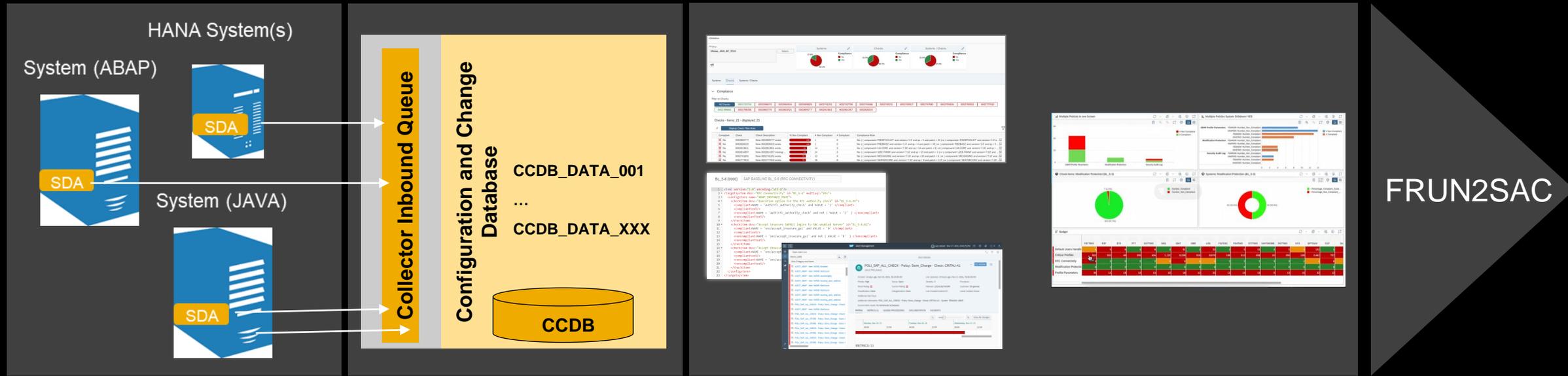


Embedded into comprehensive set of IT Operations Use Cases



Technology Foundation: SAP HANA / SAP NetWeaver ABAP + SAPUI5

From ... data ... to ... validation ... to ... dashboard



Scheduled Data Collection

Config Stores & Change History

Scheduled Policies & Alerts

Dashboard Pages

API

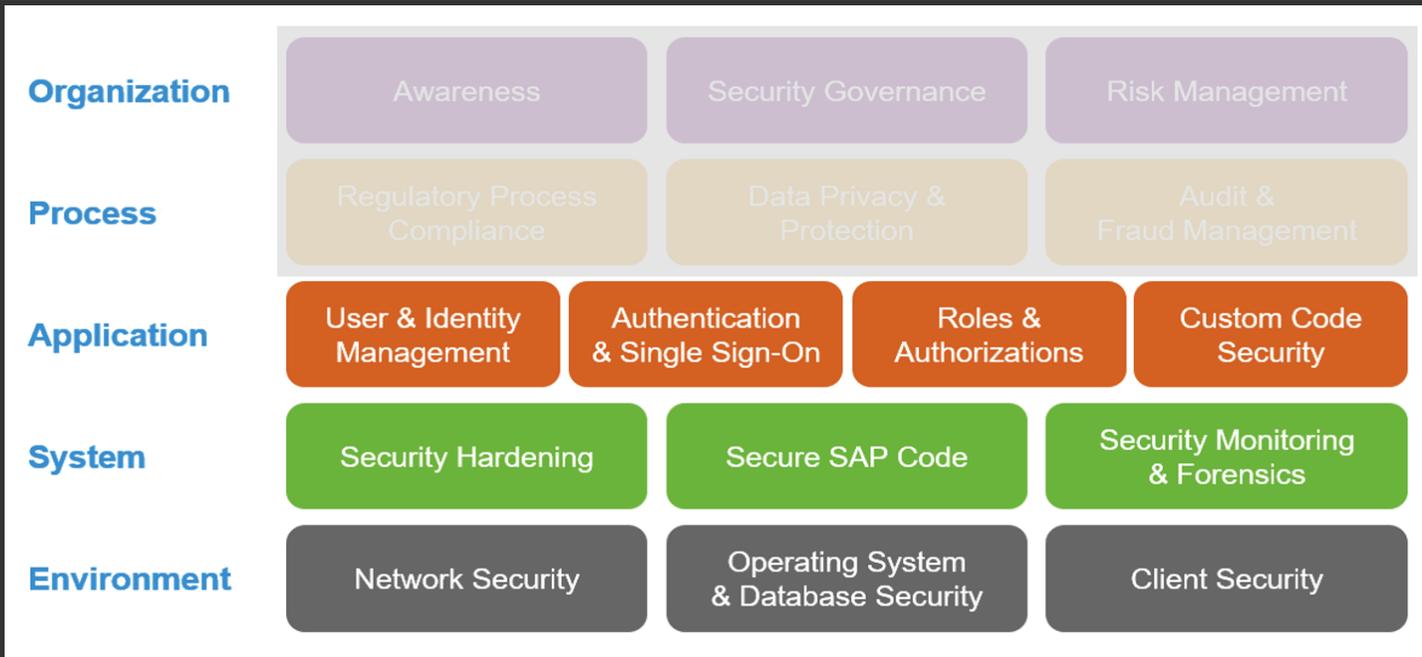
Customer Journey to Security with SAP Focused Run



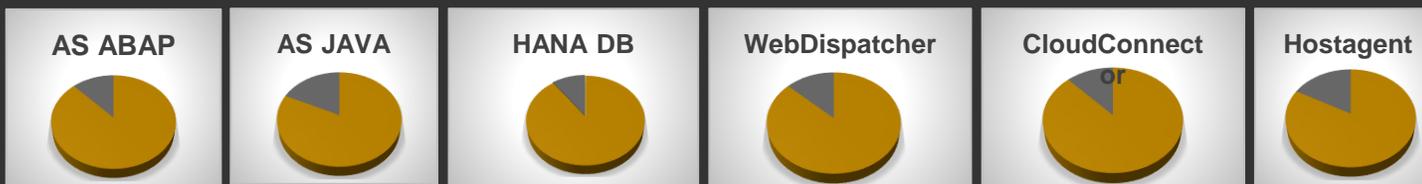
Adoption Journey – SAP Baseline

Prevent Breaches with a strong Security Baseline

Keep doors and windows closed. Have keys on a safe place. Ensure cameras are switched on...



“appropriate technical and organisational measures”



Typical Achievement with SAP Focused Run

- ✓ Automation of a comprehensive security baseline
- ✓ High coverage of common requirements
 - ✓ SAP Security Baseline Template: > 95%
 - ✓ Custom-specific Baselines: > 80%
- ✓ Stores covering old and new security features of S/4 HANA

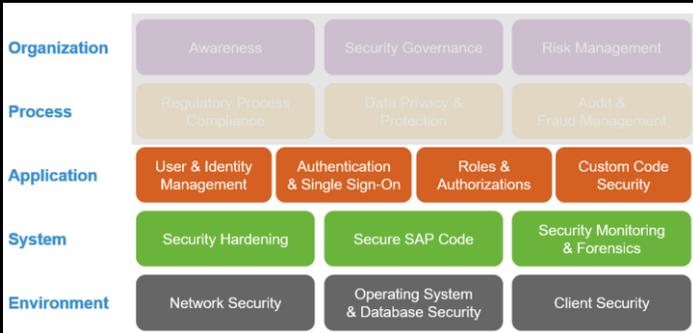
The SAP Security Baseline

Document Structure

Secure Operation Map



Document Content



User & Identity Management <ul style="list-style-type: none"> SAP Standard User 	Authentication & Single Sign-On <ul style="list-style-type: none"> Password Policy SAP Logon Tickets Password Hashes 	Roles & Authorizations <ul style="list-style-type: none"> Switchable Authorization Checks Profile Parameter & Customizing Critical Authorizations 	Security Monitoring & Forensics <ul style="list-style-type: none"> Process Logging Content Profile Parameters
Security Hardening: General <ul style="list-style-type: none"> Other Profile Parameters Modification Protection ABAP Standard User Security Store Directory Traversal Security Audit Log 	Security Hardening: Web Access <ul style="list-style-type: none"> ICM Protocols ICM Access Control ICM Usage Logging ICM Security Logging ICM Trusted Intermediate Additional ICM Profile Parameters ICM Administration Interface Web Dispatcher Configuration Limit Web Enabled Content 	Security Hardening: Common Components <ul style="list-style-type: none"> SAPStartSrv SAP Host Agent Message Server Security Enqueue Server 	Security Hardening: Communication Security <ul style="list-style-type: none"> RFC Connectivity RFC Profile Parameter RFC Trusted System Security RFC Gateway Security Securing RFC / DIAG RFC Callback RFC UCON

SAP Security Baseline Template: (SAP Note: 2253549)

Specific Technical Rules on a Detail Level

1	Overview, Requirements and Guidelines	10
1.1	Purpose of this document.....	10
2	Regulations	11
2.1	Infrastructure Security (Identifier-Prefix I)	11
2.1.1	Network Security.....	11
2.1.2	Operating System Security.....	13
2.1.3	Database Security.....	14
2.1.4	Frontend Security.....	16
2.2	Secure Code (Identifier-Prefix C)	16
2.2.1	Security Maintenance of SAP Code.....	16
2.2.2	Custom Code Security.....	16
2.3	Secure Setup (Identifier-Prefix S)	17
2.3.1	Secure Configuration.....	17
2.3.2	Communication Security.....	19
2.3.3	Data Security.....	21
2.4	Secure Operation (Identifier-Prefix O)	21
2.4.1	Users and Authorizations.....	21
2.4.2	Authentication and Single Sign-On.....	23
2.4.3	Support Security.....	23
2.4.4	Security Review and Monitoring.....	23
2.5	Security Compliance (Identifier Prefix X)	24
2.5.1	Security Governance.....	24
2.5.2	Audit.....	24
2.5.3	Cloud Security.....	24
2.5.4	Emergency Concept.....	24
3	Verifying Compliance	25
3.1	Configuration Stores	27
3.1.1	Configuration Stores for HANA based systems.....	27
3.1.2	Configuration Stores for ABAP based systems.....	27
3.1.3	Configuration Stores for Java based systems.....	28
4	Annotations and Additional Information	30
4.1	Infrastructure Security	30
4.1.1	Network Security.....	30
4.1.1.1	Network Zones and Firewalls.....	30
4.1.1.1.1	Client – Server Communication – ABAP Systems.....	31
4.1.1.1.2	Client – Server Communication – Java Systems.....	33
4.1.1.1.3	Server – Server Communication.....	34

4.1.1.2	SAP provided Gateways and Reverse Proxies and standalone components.....	34
4.1.1.2.1	SAProuter.....	35
4.1.1.2.2	SAP Web Dispatcher.....	36
4.1.1.3	Administrative Access to SAP Systems.....	37
4.1.2	Operating System Security.....	38
4.1.2.1	Windows.....	38
4.1.2.1.1	Windows Groups and Users in an SAP System Environment.....	38
4.1.2.1.2	Windows Operating System User Settings in an SAP System.....	38
4.1.2.1.3	SAP Systems in the Windows Domain Concept.....	39
4.1.2.1.4	Securing Data Relevant to the SAP System.....	39
4.1.2.1.5	Security Settings for Shared Memory.....	40
4.1.2.2	Unix.....	40
4.1.2.2.1	Protecting Specific Properties, Files and Services.....	40
4.1.2.2.2	Setting Access Privileges for SAP System Directories Under UNIX/LINUX.....	41
4.1.3	Database Security.....	41
4.1.3.1	General Recommendations.....	41
4.1.3.1.1	Authentication and Encryption.....	42
4.1.3.1.2	Authorization.....	42
4.1.3.2	SAP HANA Security.....	42
4.1.3.2.1	Change Passwords of Users after Handover.....	42
4.1.3.2.2	Deactivate SYSTEM user.....	43
4.1.3.2.3	Limit Password Lifetime.....	43
4.1.3.2.4	Password Policy.....	43
4.1.3.2.5	System privilege DATA ADMIN.....	43
4.1.3.2.6	System privileges must be Granted to Database Administrators Only.....	44
4.1.3.2.7	SQL Trace Level.....	44
4.1.3.2.8	Audit Trail.....	44
4.1.3.3	SAP MaxDB Security.....	44
4.1.3.3.1	Changing Passwords of Standard Users.....	44
4.1.3.3.2	Restricting and Checking Log Files for Failed Logon Attempts.....	45
4.1.3.3.3	Use secure Authentication.....	46
4.1.3.3.4	Implement Backup and Disaster Recovery Procedures.....	46
4.1.3.3.5	Network Split for Administrative Protocols.....	46
4.1.3.3.6	Implement Database Configuration Hardening.....	47
4.1.3.3.7	Use Dedicated Database Hosts for Productive Databases.....	47
4.1.3.3.8	Defining Clear Authorizations for Users.....	47
4.1.3.3.9	Securing Communication Channels.....	47
4.1.3.3.10	Dispensable Functions with Impact on Security.....	48
4.1.3.3.11	Checking User Input in SQL Statements.....	48
4.1.3.3.12	Trace and Log Files.....	48
4.1.3.4	Oracle.....	48
4.1.3.4.1	User Management.....	48



SAP Security Baseline Template
Version 1.9



Last update: 11/2021

Example 1: SE06 – Change Options (Configuration)

SAP System Change Option

Client Setting Cancel More

Global Setting Modifiable

Software Component	Technical Name	Modifiable
SAP Focus RUN Tool	FRUN	not modifiable (enhanceable only)
Customer Developments	HOME	Modifiable
Local Developments (No Automatic Transport)	LOCAL	Modifiable
MDG Foundation	MDG_FND	Modifiable
Foundation	S4FND	Modifiable
Cross-Application Component	SAP_ABA	restricted modifiability

Namespace/Name Range	Prefix	Modifiable
Customer Name Range		Modifiable
General SAP Name Range		Modifiable
Test Generation Namespace for BW	/1APO/	Not modifiable
	/1B0/	Not modifiable
Bank Analyzer: Generated Objects	/1BA/	Modifiable
ABAP & GUI Tools	/1BCABA/	Modifiable
Non-DDIC Objects in <sapsid> Schema for Use in AMDP	/1BCAMP/	Modifiable
ABAP Workbench	/1BCDWB/	Modifiable
Enqueue Function Groups	/1BCDWBEN/	Modifiable

Changes were saved

SAP Configuration & Security Analytics

Store Browser

Config Stores of FRNADM type Application Server ABAP - Items: 92 - displayed: 2

Description	Config Store Name	Landscape	Landscape Type	TimeStamp
Namespace change settings	NAMESPACES	FRN on vhcalthbdb	sap_bcsystem	5/19/22, 1:11 AM
Namespace change setting...	NAMESPACES_CHANGE_L...	FRN on vhcalthbdb	sap_bcsystem	5/19/22, 8:28 AM

Items

Switch table view

Namespace change settings (NAMESPACES) - Items: 139 - displayed: 139

ConfigItemKey	Value	Type of event	Valid since
NAMESPACE = /OCUST/	TEXT = Customer Name Range PREFIX = CHANGEABLE = MODIFIABLE	INITIAL	5/18/21, 1:12 AM
NAMESPACE = /OSAP/	TEXT = General SAP Name Range PREFIX = CHANGEABLE = MODIFIABLE	INITIAL	5/18/21, 1:12 AM
NAMESPACE = /1APO/	TEXT = Test Generation Namespace for BW PREFIX = /1APO/ CHANGEABLE = NOT MODIFIABLE	UPDATED	5/18/22, 7:44 PM
NAMESPACE = /1B0/	TEXT = PREFIX = /1B0/ CHANGEABLE = NOT MODIFIABLE	UPDATED	5/18/22, 7:44 PM

Example 1: SE06 – Change Options (Change Log)

SAP System Change Option

Client Setting Cancel More

Global Setting Modifiable

Software Component	Technical Name	Modifiable
SAP Focus RUN Tool	FRUN	not modifiable (enhanceable only)
Customer Developments	HOME	Modifiable
Local Developments (No Automatic Transport)	LOCAL	Modifiable
MDG Foundation	MDG_FND	Modifiable
Foundation	S4FND	Modifiable
Cross-Application Component	SAP_ABA	restricted modifiability

Namespace/Name Range	Prefix	Modifiable
Customer Name Range		Modifiable
General SAP Name Range		Modifiable
Test Generation Namespace for BW	/1APO/	Not modifiable
	/1B0/	Not modifiable
Bank Analyzer: Generated Objects	/1BA/	Modifiable
ABAP & GUI Tools	/1BCABA/	Modifiable
Non-DDIC Objects in <sapsid> Schema for Use in AMDP	/1BCAMDP/	Modifiable
ABAP Workbench	/1BCDWB/	Modifiable
Enqueue Function Groups	/1BCDWBEN/	Modifiable

Changes were saved

SAP Configuration & Security Analytics

Store Browser

Systems

Config Stores

Filter on Landscape Types

All Types sap_bcapplicationserver sap_bccentralserviceinst... sap_bcclient sap_bcsystem sap_computersystem

Config Stores of FRNADM type Application Server ABAP - Items: 92 - displayed: 5

Description	Config Store Name	Landscape	Landscape Type	TimeStamp
Clients - change log	CLIENTS_CHANGE_LOG	FRN on vhcalthdbdb	sap_bcsystem	5/18/22, 7:28 PM
Component change settings - Ch...	COMPONENTS_CHANGE_LOG	FRN on vhcalthdbdb	sap_bcsystem	5/18/22, 7:28 PM
Global change setting - Change L...	GLOBAL_CHANGE_LOG	FRN on vhcalthdbdb	sap_bcsystem	5/18/22, 7:28 PM
Logged Tables	LOGGED_TABLES	FRN on vhcalthdbdb	sap_bcsystem	5/18/22, 1:37 AM
Namespace change settings - Ch...	NAMESPACES_CHANGE_LOG	FRN on vhcalthdbdb	sap_bcsystem	5/18/22, 7:29 PM

Items

Switch table view

Namespace change settings - Change log (NAMESPACES_CHANGE_LOG) - Items: 2 - displayed: 2

Date Range: 1/16/22 To 5/18/22

ConfigitemKey	Value	Type of event	Valid since
COMPONENT = /1APO/	PREVIOUS = Modifiable AFTERWARDS = Not Modifiable CHANGEUSER = MUELLERHEN EVENT_TIMESTAMP = 20220518173902	EVENT	5/18/22, 7:39 PM
COMPONENT = /1B0/	PREVIOUS = Modifiable AFTERWARDS = Not Modifiable CHANGEUSER = MUELLERHEN EVENT_TIMESTAMP = 20220518173902	EVENT	5/18/22, 7:39 PM

Policies – SAP Recommended and Custom Validations

- ✓ **Build your own** validation policies **or get them ready-to-use** as SAP Service (Github or tailor-made)
- ✓ Report on what you actually are able to **get clean** and **keep clean**

1 Security Policy Document

2.3.2 Communication Security

S-6: RFC Connectivity

- a) All RFC destinations must be required and must be assigned to an owner responsible for the destination and who can provide information on the need and usage of this destination. RFC destinations not or no longer required must be removed.
- b) RFC destinations with stored user credentials or using trusted system logon must only exist between systems of the same security classification or from system of higher security classification to systems of lower security classification.
- c) The RFC authorization check has to be activated with the system profile parameter `auth/rfc_authority_check`. This parameter must be set to the value '1'.
- d) Systems of higher security classification may never trust systems of lower security classification.

- e) If a SAP system technically allows for the use of UCON, then UCON should be activated and RFC services not required should be switched off through UCON.
- f) The inbound RFC or GUI connections have to be encrypted. Use the parameters `snc/accept_insecure_gui` or `snc/accept_insecure_rfc` to make sure that the logon inbound connection is secured with SNC.

2 Policy Definition is an XML file

```

BL_S-6 [0000]  SAP BASELINE BL_S-6 (RFC CONNECTIVITY)
1 <?xml version="1.0" encoding="utf-8"?>
2 <targetssystem desc="RFC Connectivity" id="BL_S-6" multisql="Yes">
3   <configstore name="ABAP_INSTANCE_PAHI">
4     <checkitem desc="Execution option for the RFC authority check" id="BL_S-6.01">
5       <compliant>NAME = 'auth/rfc_authority_check' and VALUE = '1' </compliant>
6       <complianttext/>
7       <noncompliant>NAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) </noncompliant>
8       <noncomplianttext/>
9     </checkitem>
10    <checkitem desc="Accept insecure SAPGUI logins to SNC-enabled Server" id="BL_S-6.02">
11      <compliant>NAME = 'snc/accept_insecure_gui' and VALUE = '0' </compliant>
12      <complianttext/>
13      <noncompliant>NAME = 'snc/accept_insecure_gui' and not ( VALUE = '0' ) </noncompliant>
14      <noncomplianttext/>
15    </checkitem>
16    <checkitem desc="Accept insecure RFC-connections to SNC-enabled Server" id="BL_S-6.03">
17      <compliant>NAME = 'snc/accept_insecure_rfc' and VALUE = '0' </compliant>
18      <complianttext/>
19      <noncompliant>NAME = 'snc/accept_insecure_rfc' and not ( VALUE = '0' ) </noncompliant>
20      <noncomplianttext/>
21    </checkitem>
22  </configstore>
23 </targetssystem>
  
```

3 Validation Result

Compliance of systems

Policy ID: BASELINE SAP POLICY S-6 (ABAP RFC CONNECTIVITY) (X)

3 Validated Systems | 3 Non Compliant | 0 Compliant

Compliant	C.	System ID	System	% Non Compliant	# Non Compliant	# Compliant
✗	No	S	FTACDM Applicat	50	1	1
✗	No	N	SQLNZE Applicat	50	1	1
✗	No	S	QPTSSC Applicat	50	2	2

Policy Definition BASELINE SAP POLICY S-6 (ABAP RFC CONNECTIVITY) (X) (Exemptions applied) - QPTSSC type Application Server ABAP - Items: 4

Compliant	Landscape	Check	Check Description	Configuration Item	Value	Rule
✗ No	AppServer 09 of QPT o...	BL_S-6.03	Accept insecure RFC-connections to SNC-enabled ...	NAME = snc/accept_insecure_rfc	VALUE = 1	NAME = 'snc/accept_insecure_rfc' and not (VALUE = ...
✗ No	AppServer 09 of QPT o...	BL_S-6.03	Accept insecure RFC-connections to SNC-enabled ...	NAME = snc/accept_insecure_rfc	VALUE = 1	NAME = 'snc/accept_insecure_rfc' and not (VALUE = ...
✓ Yes	AppServer 09 of QPT o...	BL_S-6.01	Execution option for the RFC authority check	NAME = auth/rfc_authority_check	VALUE = 1	NAME = 'auth/rfc_authority_check' and VALUE = '1'
✓ Yes	AppServer 09 of QPT o...	BL_S-6.01	Execution option for the RFC authority check	NAME = auth/rfc_authority_check	VALUE = 1	NAME = 'auth/rfc_authority_check' and VALUE = '1'

Views on Validation and Trendanalysis

Validation

Policy: SEC_JAVA_BC_2019

Systems: 17.6% Compliance 82.4%

Checks: 33.3% Compliance 46.7%

Systems / Checks: 32.6% Compliance 17.4%

Compliance of systems

Technical Systems - Items: 17

Compliant	Customer	System ID	System Type	% Non Compliant	# Non Compliant	# Compliant	IT Admin Role	Lifecycle Status
No	SDN	MAKSDA	Application Server Java	100%	11	0	Production System	Active
No	SDN	SOUZOH	Application Server Java	100%	11	0	Production System	Active
No	T-Mobile Business	JCTMDO	Application Server Java	100%	11	0	Production System	Inactive
No	T-Mobile Business	JCTMDO	Application Server Java	100%	11	0	Production System	Active
No	T-Mobile Business	SDJ	Application Server Java	100%	11	0	Undefined	Active
No	DLM	MEJ	Application Server Java	100%	10	1	Undefined	Active

Validation

Policy: SEC_JAVA_BC_2019

Systems: 17.6% Compliance 82.4%

Checks: 33.3% Compliance 46.7%

Systems / Checks: 32.6% Compliance 17.4%

Compliance

Filter on Checks

Checks - Items: 21 - displayed: 21

Compliant	Check	Check Description	% Non Compliant	# Non Compliant	# Compliant	Compliance Rule
No	0002089777	Note 0002089777 exists	100%	1	0	No: ((component='PIB2BT00LKIT' and version='1.0' and sp = 5 and patch = 45) or (component='PIB2BT00LKIT' and version='1.0' and sp = 5 and patch = 26) or (component='PIB2BASZ' and version='1.0' and sp = 14 and patch = 35) or (component='PIB2BASZ' and version='1.0' and sp = 5 and patch = 1) or (component='LM-CORE' and version='7.30' and sp = 14 and patch < 6) or (component='LM-CORE' and version='7.30' and sp = 14 and patch = 6) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch < 1) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch = 1) or (component='MESSAGING' and version='7.10' and sp = 20 and patch < 6) or (component='MESSAGING' and version='7.10' and sp = 20 and patch = 6) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch < 137) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch = 137)
No	0002082015	Note 0002082015 exists	100%	1	0	No: ((component='PIB2BASZ' and version='1.0' and sp = 14 and patch < 35) or (component='PIB2BASZ' and version='1.0' and sp = 5 and patch = 1) or (component='LM-CORE' and version='7.30' and sp = 14 and patch < 6) or (component='LM-CORE' and version='7.30' and sp = 14 and patch = 6) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch < 1) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch = 1) or (component='MESSAGING' and version='7.10' and sp = 20 and patch < 6) or (component='MESSAGING' and version='7.10' and sp = 20 and patch = 6) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch < 137) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch = 137)
No	00020813811	Note 00020813811 exists	100%	14	3	No: ((component='PIB2BASZ' and version='1.0' and sp = 14 and patch < 35) or (component='PIB2BASZ' and version='1.0' and sp = 5 and patch = 1) or (component='LM-CORE' and version='7.30' and sp = 14 and patch < 6) or (component='LM-CORE' and version='7.30' and sp = 14 and patch = 6) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch < 1) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch = 1) or (component='MESSAGING' and version='7.10' and sp = 20 and patch < 6) or (component='MESSAGING' and version='7.10' and sp = 20 and patch = 6) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch < 137) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch = 137)
No	00020814357	Note 00020814357 missing	100%	14	3	No: ((component='PIB2BASZ' and version='1.0' and sp = 14 and patch < 35) or (component='PIB2BASZ' and version='1.0' and sp = 5 and patch = 1) or (component='LM-CORE' and version='7.30' and sp = 14 and patch < 6) or (component='LM-CORE' and version='7.30' and sp = 14 and patch = 6) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch < 1) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch = 1) or (component='MESSAGING' and version='7.10' and sp = 20 and patch < 6) or (component='MESSAGING' and version='7.10' and sp = 20 and patch = 6) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch < 137) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch = 137)
No	0002741201	Note 0002741201 exists	100%	13	4	No: ((component='PIB2BASZ' and version='1.0' and sp = 14 and patch < 35) or (component='PIB2BASZ' and version='1.0' and sp = 5 and patch = 1) or (component='LM-CORE' and version='7.30' and sp = 14 and patch < 6) or (component='LM-CORE' and version='7.30' and sp = 14 and patch = 6) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch < 1) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch = 1) or (component='MESSAGING' and version='7.10' and sp = 20 and patch < 6) or (component='MESSAGING' and version='7.10' and sp = 20 and patch = 6) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch < 137) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch = 137)
No	0002777910	Note 0002777910 exists	100%	20	6	No: ((component='PIB2BASZ' and version='1.0' and sp = 14 and patch < 35) or (component='PIB2BASZ' and version='1.0' and sp = 5 and patch = 1) or (component='LM-CORE' and version='7.30' and sp = 14 and patch < 6) or (component='LM-CORE' and version='7.30' and sp = 14 and patch = 6) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch < 1) or (component='ZEE-FRMW' and version='7.10' and sp = 23 and patch = 1) or (component='MESSAGING' and version='7.10' and sp = 20 and patch < 6) or (component='MESSAGING' and version='7.10' and sp = 20 and patch = 6) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch < 137) or (component='SERVERCORE' and version='7.20' and sp = 9 and patch = 137)

Validation

Policy: SEC_JAVA_BC_2019

Systems: 17.6% Compliance 82.4%

Checks: 33.3% Compliance 46.7%

Systems / Checks: 32.6% Compliance 17.4%

Compliance

Checks - Items: 17

System ID	System Type	IT Admin Role	Lifecycle Status	0001715734	0002286679	0002664504	0002689925	0002741201	0002742758	0002744086	0002745211	0002745917	0002747683	0002755438	0002779502	0002777910
FBTMO	JAVA	Production Syst...	Active	<input type="checkbox"/>												
FJTTMO	JAVA	Development S...	Active	<input type="checkbox"/>												
MEJ	JAVA	Undefined	Active	<input type="checkbox"/>												
JTJ	JAVA	Undefined	Active	<input type="checkbox"/>												
JCTMDO	JAVA	Production Syst...	Inactive	<input type="checkbox"/>												
JCTMDO	JAVA	Production Syst...	Active	<input type="checkbox"/>												
JSK	JAVA	Undefined	Active	<input type="checkbox"/>												
MAKSDA	JAVA	Production Syst...	Active	<input type="checkbox"/>												
MEJ	JAVA	Undefined	Active	<input type="checkbox"/>												

SAP CSA - Trend Analysis

Trend Analysis - Policies

Table of Policies scheduled for Trend: 1

Time Frame Selection 8/11/21, 3:35 PM - 11/11/21, 3:35 PM

Percentage of Non Compliant

Policy	Description	Type	Trend % of Non Compliant	Slope	Frequency for Calculation	First avail. Validation
SEC_JAVA_HIGH+BASE	SEC_JAVA_HIGH+BASE	Single	Up	0.22	WEEK	9/22/21, 7:17 AM

Policy SEC_JAVA_HIGH+BASE

Percentage of Non Compliant

Year	Percentage of Non Compliant
202132	26.25
202133	26.00
202134	25.00
202135	24.38
202136	31.27
202137	30.93
202138	30.67
202139	30.12
202140	29.24
202141	29.56
202142	28.78
202143	28.31
202144	28.55
202145	28.09

Systems

Table of Systems; Policy: SEC_JAVA_HIGH+BASE; Items: 74 - displayed: 74; Up: 51; Down: 21

Percentage of Non Compliant

Policy	D...	Trend % of Non Compliant	Slope	# Non Compliant Latest	Cus...	System ID	System Type	IT Admin Role	Lifecycle Status	System Attributes
SEC_JAVA_	SE...	Up	4.24	37	INT	...	JAVA	Test System	Active	EXTENDED_SID =
SEC_JAVA_	SE...	Steady	0.00	22	INT	...	JAVA	Production System	Active	EXTENDED_SID =
SEC_JAVA_	SE...	Up	0.81	15	DMZ	...	JAVA	Test System	Active	EXTENDED_SID =
SEC_JAVA_	SE...	Up	0.84	9	DMZ	...	JAVA	Test System	Active	EXTENDED_SID =
SEC_JAVA_	SE...	Up	1.08	8	INT	...	JAVA	Production System	Active	EXTENDED_SID =
SEC_JAVA_	SE...	Down	-2.28	13	INT	...	JAVA	Development System	Active	EXTENDED_SID =
SEC_JAVA_	SE...	Up	0.76	19	INT	...	JAVA	Undefined	Active	EXTENDED_SID =

Systems [%]

Systems [Time]

Create Alerts from Policies and Store Changes Examples

Alert Definitions for Policies

Alert Definitions for Policies - Items: 8

Alert ID	Alert Description	Frequency	Aggregation Level
ABAP_SNOTES_2021	FHJLQ	Daily	System
AUDIT_ABAP	Mandatory Audit Log Configuration changed or	Daily	Item
AUDIT_HANA	Mandatory HANA Audit Log Configuration changed	Daily	Item
CRITAU_ABAP	New User with critical authorization detected	Daily	Store
HOTNEWS_ABAP	Security of priority HOTNEWS not deployed in A	Daily	System
SE06_CLIENT_CHANGE	SE06 Client Change options got changed (any	Hourly	System
SE06_NAMESPACE	SE06 Change Options for at least 1 Namespac	Hourly	System
ZSAP_CPI_POLICY	Cloud Platform Integration - Certificates	Daily	System

Change Alert Definition

Alert ID
SE06_NAMESPACE

*Alert Description
SE06 Change Options for at least 1 Namespace have been changed within last 24 hours

Policy:
SE06_Settings

Aggregation Level
System

Type of Scope
All

Frequency
Hourly

Severity
9 - Critical

Active

Save Cancel

Define Alert

*Alert ID
SE06_CLIENT_CHANGE

*Alert Description
SE06 Client Change options got changed (any detected change in the Config Store)

Alert Source
Store content Change

*Select a Config Store..
CLIENTS_CHANGE_LOG//S00310

Aggregation Level
System

Type of Scope
All

Frequency
Hourly

Severity
7

Active

Save Cancel

CSA Alert Processing

Alert Management | Last refresh : May 19, 2022, 9:33:34 AM

Open Alert List

Alerts (14)

Alert Category and Name

- SE06_NAMESPACE - Policy: SE06_Setting
- CRITAU_ABAP - CSA Store Change - Store
- AUDIT_ABAP - Item: NAME=SlotCount
- AUDIT_HANA - Item: item=no data found
- AUDIT_HANA - Item: item=no data found
- AUDIT_ABAP - Item: NAME=rsau/log_peer
- AUDIT_ABAP - Item: NAME=rsau/log_peer
- AUDIT_ABAP - Item: NAME=Enabled
- AUDIT_ABAP - Item: NAME=SlotCount
- AUDIT_ABAP - Item: NAME=rsau/integrity
- ABAP_SNOTES_2021 - Policy: 2021_SNot
- HOTNEWS_ABAP - Policy: 2021_HOTNEW
- HOTNEWS_ABAP - Policy: 2021_HOTNEW
- ABAP_SNOTES_2021 - Policy: 2021_SNot

Alert Details

SE06_NAMESPACE - Policy: SE06_Settings - System
FRNADM [Application Server ABAP]

Created: 12 hours ago, May 18, 2022, 09:10:01 PM | Last Updated: 24 mins ago, May 19, 2022, 09:10:01 AM

Priority: Very high | Status: Open | Severity: 9 | Processor:

Worst Rating: ⊗ | Current Rating: ⊗ | Network: LOCALNETWO RK | Customer: Oil general

Classification: None | Categorization: None | Last Created Incident ID: | Latest Incident Status:

Additional Alert Keys:

Additional Information: SE06_NAMESPACE - Policy: SE06_Settings - System - System: FRNADM-ABAP.

Current Work mode: No Workmode Scheduled

RATING | METRICS (1) | GUIDED PROCEDURES | DOCUMENTATION | INCIDENTS

Thursday, May 19, 22

20:00 22:00 00:00 02:00 04:00 06:00 08:00

Alert Details

SE06_NAMESPACE - Policy: SE06_Settings - System
FRNADM [Application Server ABAP]

RATING | METRICS (1) | GUIDED PROCEDURES | DOCUMENTATION | INCIDENTS

METRICS (1)

From: May 18, 2022 09:10:01 PM | To: May 19, 2022 09:10:01 AM | Metric Default View

Metric Name	First	Worst	Last	Min	Max	Last Value	Last Text
SE06_NAMESPACE - Policy: SE0...	⊗	⊗	⊗	4	4	4	# Non compliant items

GUIDED PROCEDURES

Guided Procedure Name	Processing Status	Last Changed By	Last Changed On	Result Report
No Guided Procedures assigned				

DOCUMENTATION

SE06 Change Options for at least 1 Namespace have been changed within last 24 hours
Non compliant items found: 4 - Compliant items found: 2 - All items found: 6 - System: FRNADM-ABAP.

CSA Validation

The Configuration & Security Analytics validation does check configuration items related to definition of a policy.

Alert Description

A red alert indicates that there is a least one item that does not fulfill the rule defined in the policy.

Error Analysis

For checking which items do not fulfill the rule follow this link to the CSA validation:
[Configuration & Security Analytics - Validation](#)

INCIDENTS

Alert provides a link to CSA Validation Result for further details

SAP Configuration & Security Analytics

Validation

*Policy: SE06_Settings

Validated at 5/19/2022, 9:30:07 AM - Less than 1 hour ago

Systems

0.0% Compliance
100.0%

Check Items

33.3% Compliance
66.7%

Systems / Checks

0.0% Compliance
100.0%

Systems Checks Systems / Checks

Compliance

Checks - Items: 1 - displayed: 1

Display Check Filter Area

Compliant	Policy	Check	Check Description	% Non Compliant	# Non Compliant	# Compliant	Compliance Rule
No	SE06_Settings	SE06_1	[p1-critical] Namespaces (Change Options)	67	4	2	No: NonCompliance Rule: (component like '%' and previo...

Items

Check SE06_Settings - SE06_1 - Items: 4

Display only Items that have Compliant = No

Compliant	System ID	System Type	Landscape	Configuration Item	Value	Valid since
No	FRNADM	Application Server A...	FRN on vhcathbdb	COMPONENT = /1DH/	PREVIOUS = Not Modifiable AFTERWARDS = Modifiable CHANGEUSER = DDIC	12/15/21, 7:44 PM
No	FRNADM	Application Server A...	FRN on vhcathbdb	COMPONENT = /MFND/	PREVIOUS = Not Modifiable AFTERWARDS = Modifiable CHANGEUSER = DDIC	12/15/21, 7:44 PM
No	FRNADM	Application Server A...	FRN on vhcathbdb	COMPONENT = /SMFND/	PREVIOUS = Not Modifiable AFTERWARDS = Modifiable CHANGEUSER = DDIC	12/15/21, 7:44 PM
No	FRNADM	Application Server A...	FRN on vhcathbdb	COMPONENT = /SYCLO/	PREVIOUS = Not Modifiable AFTERWARDS = Modifiable CHANGEUSER = DDIC	12/15/21, 7:44 PM

Adoption Journey – SAP Security Notes

Example 2: SAP Security Notes Validation

After each SAP PatchDay

22 Document(s) To Be Reviewed

SAP Component	Number	Title	CVSS Score	CVSS Vector	Category	Priority	Released On	First Released On
XX-SER-SN	3170990	[CVE-2022-22965] Central Security Note for Remote Code Execution vulnerability associated with Spring Framework	9,8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	10.05.2022	12.04.2022
BI-BIP-INS	2998510	[CVE-2022-28214] Central Management Server Information Disclosure in Business Intelligence Update	7,8	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Program error	Correction with high priority	10.05.2022	10.05.2022
SBO-CRO-SEC	3189409	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Business One Cloud	9,8	CVSS:/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	10.05.2022	10.05.2022
BC-CST-WDP	3145046	[CVE-2022-27656] Cross-Site Scripting (XSS) vulnerability in administration UI of SAP Webdispatcher and SAP Netweaver AS for ABAP and Java (ICM)	8,3	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H	Program error	Correction with high priority	10.05.2022	10.05.2022
CEC-COM-CP5...	3171258	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Commerce	9,8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	18.04.2022	18.04.2022
IS-T-MA	3189635	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Customer Profitability Analytics	9,8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	14.04.2022	14.04.2022
IS-SE-CCO	3187290	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Customer Checkout	9,8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	12.04.2022	12.04.2022
BC-SYB-PD	3189429	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in PowerDesigner Web (upto including 16.7 SPO5 PLO1)	9,8	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Program error	HotNews	12.04.2022	12.04.2022
MFG-MI	3158613	Update 1 to Security Note 3022622 - [CVE-2021-21480] Code injection vulnerability in SAP Manufacturing Integration and Intelligence	9,1	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	Program error	HotNews	12.04.2022	12.04.2022

<https://launchpad.support.sap.com/#/securitynotes>

Validation Results Summary:

- Systems of PatchDay: 2022-05 (all HIGH and HOTNEWS)
- States of PatchDay: 2022-04 (all High and Hotnews)
- Validated at: 5/16/2022, 11:39:36 AM - Less than 1 hour ago

Compliance Status:

- 40.7% Compliance (Yes)
- 59.3% Compliance (No)

Systems / Checks: 77 items

Customer	System ID	System Type	IT Admin Role	Lifecycle Status	2022-05_ALL_p1...	2022-04_ALL_p1...	2022-04...	2022-04...	2022-04...	2022-04...									
T-Mobile Business	FBUTMO	JAVA	Production System	Active															
T-Mobile Business	FDUTMO	ABAP	Quality Assurance Sy...	Active															
T-Mobile Business	HSUTMO	JAVA	Production System	Active															
T-Mobile Business	S4UTMO08	ABAP	Production System	Active															
T-Mobile Business	PCUTMO	JAVA	Production System	Active															
T-Mobile Business	FACTMO	ABAP	Undefined	Active															
DLM	QADLM	ABAP	Undefined	Active															
DLM	GOA	ABAP	Undefined	Active															
T-Mobile Business	RHWGVS	HANA08	Undefined	Active															
T-Mobile Business	RHM	HANA08	Undefined	Active															
T-Mobile Business	CCWTHO	BOEJ	Production System	Active															
IBM	U295M	JAVA	Undefined	Active															
DLM	N7S	JAVA	Undefined	Active															
T-Mobile Business	SO4TMO	ABAP	Undefined	Active															
DLM	OEJ	JAVA	Undefined	Active															
MPS	H5U	JAVA	Undefined	Active															
MPS	HAD	ABAP	Undefined	Active															
IBM	V3J	JAVA	Undefined	Active															
DLM	N2DLM	JAVA	Production System	Active															
T-Mobile Business	JCRTHO	JAVA	Production System	Undefined															
DLM	JCSJRT	JAVA	Production System	Active															
SAP Focused Run ...	FO4ADM	ABAP	Production System	Active															
T-Mobile Business	H54TMO	ABAP	Undefined	Active															

SAP Focused Run Validation Result

Files in repository:

- ABAP_patchday_2022_01.xml
- ABAP_patchday_2022_02.xml
- ABAP_patchday_2022_03.xml
- ABAP_patchday_2022_04.xml
- ABAP_patchday_2022_05.xml
- ABAP_patchday_2022_06.xml
- ABAP_patchday_2022_07.xml
- ABAP_patchday_2022_08.xml
- ABAP_patchday_2022_09.xml
- ABAP_patchday_2022_10.xml
- ABAP_patchday_2022_11.xml
- ABAP_patchday_2022_12.xml
- ABAP_patchday_2023_01.xml
- ABAP_patchday_2023_02.xml
- ABAP_patchday_2023_03.xml
- ABAP_patchday_2023_04.xml
- ABAP_patchday_2023_05.xml
- ABAP_patchday_2023_06.xml
- ABAP_patchday_2023_07.xml
- ABAP_patchday_2023_08.xml
- ABAP_patchday_2023_09.xml
- ABAP_patchday_2023_10.xml
- ABAP_patchday_2023_11.xml
- ABAP_patchday_2023_12.xml
- ABAP_patchday_2024_01.xml
- ABAP_patchday_2024_02.xml
- ABAP_patchday_2024_03.xml
- ABAP_patchday_2024_04.xml
- ABAP_patchday_2024_05.xml
- ABAP_patchday_2024_06.xml
- ABAP_patchday_2024_07.xml
- ABAP_patchday_2024_08.xml
- ABAP_patchday_2024_09.xml
- ABAP_patchday_2024_10.xml
- ABAP_patchday_2024_11.xml
- ABAP_patchday_2024_12.xml
- ABAP_patchday_2025_01.xml
- ABAP_patchday_2025_02.xml
- ABAP_patchday_2025_03.xml
- ABAP_patchday_2025_04.xml
- ABAP_patchday_2025_05.xml
- ABAP_patchday_2025_06.xml
- ABAP_patchday_2025_07.xml
- ABAP_patchday_2025_08.xml
- ABAP_patchday_2025_09.xml
- ABAP_patchday_2025_10.xml
- ABAP_patchday_2025_11.xml
- ABAP_patchday_2025_12.xml
- ABAP_patchday_2026_01.xml
- ABAP_patchday_2026_02.xml
- ABAP_patchday_2026_03.xml
- ABAP_patchday_2026_04.xml
- ABAP_patchday_2026_05.xml
- ABAP_patchday_2026_06.xml
- ABAP_patchday_2026_07.xml
- ABAP_patchday_2026_08.xml
- ABAP_patchday_2026_09.xml
- ABAP_patchday_2026_10.xml
- ABAP_patchday_2026_11.xml
- ABAP_patchday_2026_12.xml
- ABAP_patchday_2027_01.xml
- ABAP_patchday_2027_02.xml
- ABAP_patchday_2027_03.xml
- ABAP_patchday_2027_04.xml
- ABAP_patchday_2027_05.xml
- ABAP_patchday_2027_06.xml
- ABAP_patchday_2027_07.xml
- ABAP_patchday_2027_08.xml
- ABAP_patchday_2027_09.xml
- ABAP_patchday_2027_10.xml
- ABAP_patchday_2027_11.xml
- ABAP_patchday_2027_12.xml
- ABAP_patchday_2028_01.xml
- ABAP_patchday_2028_02.xml
- ABAP_patchday_2028_03.xml
- ABAP_patchday_2028_04.xml
- ABAP_patchday_2028_05.xml
- ABAP_patchday_2028_06.xml
- ABAP_patchday_2028_07.xml
- ABAP_patchday_2028_08.xml
- ABAP_patchday_2028_09.xml
- ABAP_patchday_2028_10.xml
- ABAP_patchday_2028_11.xml
- ABAP_patchday_2028_12.xml
- ABAP_patchday_2029_01.xml
- ABAP_patchday_2029_02.xml
- ABAP_patchday_2029_03.xml
- ABAP_patchday_2029_04.xml
- ABAP_patchday_2029_05.xml
- ABAP_patchday_2029_06.xml
- ABAP_patchday_2029_07.xml
- ABAP_patchday_2029_08.xml
- ABAP_patchday_2029_09.xml
- ABAP_patchday_2029_10.xml
- ABAP_patchday_2029_11.xml
- ABAP_patchday_2029_12.xml
- ABAP_patchday_2030_01.xml
- ABAP_patchday_2030_02.xml
- ABAP_patchday_2030_03.xml
- ABAP_patchday_2030_04.xml
- ABAP_patchday_2030_05.xml
- ABAP_patchday_2030_06.xml
- ABAP_patchday_2030_07.xml
- ABAP_patchday_2030_08.xml
- ABAP_patchday_2030_09.xml
- ABAP_patchday_2030_10.xml
- ABAP_patchday_2030_11.xml
- ABAP_patchday_2030_12.xml

ABAP / HANA from GitHub (SAP-Samples)

Policy Maintenance: Single Policies

Policy Name	Version	Description	Generated	Schedule	Changed by	Changed at	Active Exemptions
2022-05_ALL_p1p2	0000	SNotes of PatchDay: 2022-05 (all HIGH and HOTNEWS)	✓	Off	MUELLERHEN	5/10/2022, 7:53:29 PM	0
2022-04_ALL_p1p2	0000	SNotes of PatchDay: 2022-04 (All High and Hotnews)	✓	Off	MUELLERHEN	5/11/2022, 5:40:12 PM	0

SNotes of PatchDay: 2022-05 (all HIGH and HOTNEWS)

```

2022-05_ALL_p1p2 [0000]
1 <?xml version="1.0" encoding="utf-8"?>
2 <!--
3 This FRUN CSA policy contains rules to check the following (Priority HIGH, HOTNEWS) Security Notes:
4
5 ABAP KERNEL
6 [2-CVSS 8.3] 3145046 BC-CST-WDP - [CVE-2022-27656] Cross-Site Scripting (XSS) vulnerability in administration UI of SAP Webdispatcher and SAP Netweaver AS for ABAP and Java (ICM) (Version 11)
7 JAVA KERNEL
8 [2-CVSS 8.3] 3145046 BC-CST-WDP - [CVE-2022-27656] Cross-Site Scripting (XSS) vulnerability in administration UI of SAP Webdispatcher and SAP Netweaver AS for ABAP and Java (ICM) (Version 11)
9 SAP WEBDISPATCHER
10 [2-CVSS 8.3] 3145046 BC-CST-WDP - [CVE-2022-27656] Cross-Site Scripting (XSS) vulnerability in administration UI of SAP Webdispatcher and SAP Netweaver AS for ABAP and Java (ICM) (Version 11)
11 BOEJ Platform
12 [2-CVSS 7.8] 2998510 BI-BIP-INS - [CVE-2022-28214] Central Management Server Information Disclosure in Business Intelligence Update (Version 5)

```

Security Notes (High, Hotnews) – Coverage with SAP Focused Run

Recent Examples (Excel-Download from <https://launchpad.support.sap.com/#/securitynotes>)

May '22

Numbe	Title	CVSS Sc	CVSS V	Priority	Released	First Released	Comment
3170990	[CVE-2022-22965] Central Security Note for Remote Code Execu	9,8	CVSS:3.0//	HotNews	10.05.2022	12.04.2022	Collective note (Spring Framework)
2998510	[CVE-2022-28214] Central Management Server Information Dis	7,8	CVSS:3.0//	Correction with high priority	10.05.2022	10.05.2022	BOBI Platform
3189409	[CVE-2022-22965] Remote Code Execution vulnerability associa	9,8	CVSS:/AV:	HotNews	10.05.2022	10.05.2022	Business One
3145046	[CVE-2022-27656] Cross-Site Scripting (XSS) vulnerability in adm	8,3	CVSS:3.0//	Correction with high priority	10.05.2022	10.05.2022	Webdispatcher, ABAP, JAVA
3171258	[CVE-2022-22965] Remote Code Execution vulnerability associa	9,8	CVSS:3.0//	HotNews	18.04.2022	18.04.2022	Hybris Commerce
3189635	[CVE-2022-22965] Remote Code Execution vulnerability associa	9,8	CVSS:3.0//	HotNews	14.04.2022	14.04.2022	(XSA App) MTA TELCO BIG DATA CORE 2.0

April '22

Numbe	Title	CVSS Sc	CVSS V	Priority	Released	First Released	Type
3187290	[CVE-2022-22965] Remote Code Execution vulnerability associa	9,8	CVSS:3.0//	HotNews	12.04.2022	12.04.2022	native JAVA Application (BTP)
3189429	[CVE-2022-22965] Remote Code Execution vulnerability associa	9,8	CVSS:3.0//	HotNews	12.04.2022	12.04.2022	native JAVA Application (Sybase)
3158613	Update 1 to Security Note 3022622 - [CVE-2021-21480] Code in	9,1	CVSS:3.0//	HotNews	12.04.2022	12.04.2022	JAVA
3155609	Privilege escalation vulnerability in Apache Tomcat server com	7	CVSS:3.0//	Correction with high priority	12.04.2022	12.04.2022	Hybris Commerce
3130497	[CVE-2022-27671] CSRF token visible in one of the URL in SAP B	8,2	CVSS:/AV:	Correction with high priority	12.04.2022	12.04.2022	BO BI Platform
3111311	[CVE-2022-28772] Denial of service (DOS) in SAP Web Dispatch	7,5	CVSS:3.0//	Correction with high priority	12.04.2022	12.04.2022	Kernel, WebD, XSA, XSC
3022622	[CVE-2021-21480] Code injection vulnerability in SAP Manufact	9,1	CVSS:3.0//	HotNews	12.04.2022	09.03.2021	JAVA
2622660	Security updates for the browser control Google Chromium de	10	CVSS:3.0//	HotNews	12.04.2022	10.04.2018	Business Client
3189428	[CVE-2022-22965] Remote Code Execution vulnerability associa	9,8	CVSS:3.0//	HotNews	12.04.2022	12.04.2022	HANA (XSA)
3170990	[CVE-2022-22965] Central Security Note for Remote Code Execu	9,8	CVSS:3.0//	HotNews	12.04.2022	12.04.2022	Collective Note
3123396	[CVE-2022-22536] Request smuggling and request concatenati	10	CVSS:3.0//	HotNews	22.03.2022	08.02.2022	Kernel, WebD
3123427	[CVE-2022-22532] HTTP Request Smuggling in SAP NetWeaver	10	CVSS:3.0//	Correction with high priority	22.03.2022	08.02.2022	JAVA
3080567	[CVE-2021-38162] HTTP Request Smuggling in SAP Web Dispatc	8,9	CVSS:3.0//	Correction with high priority	22.03.2022	14.09.2021	Kernel/WebDispatcher
3149805	[CVE-2022-26101] Cross-Site Scripting (XSS) vulnerability in SAP	8,2	CVSS:3.0//	Correction with high priority	22.03.2022	08.03.2022	ABAP

March '22

Numbe	Title	CVSS Sc	CVSS V	Priority	Released	First Released	Type
3131047	[CVE-2021-44228] Central Security Note for Remote Code Exe	10	CVSS:3.0//	HotNews	08.03.2022	15.12.2021	Collective Note (Log4j)
3154684	[CVE-2021-44228] Remote Code Execution vulnerability associa	10	CVSS:3.0//	HotNews	08.03.2022	08.03.2022	Mobile
3149805	[CVE-2022-26101] Cross-Site Scripting (XSS) vulnerability in SA	8,1	CVSS:3.0//	Correction with high priority	08.03.2022	08.03.2022	ABAP
3145987	[CVE-2022-24396] Missing Authentication check in SAP Focuse	9,3	CVSS:3.0//	HotNews	08.03.2022	08.03.2022	Hostagent / Simple Diagnostic Agent
3123396	[CVE-2022-22536] Request smuggling and request concatenati	10	CVSS:3.0//	HotNews	08.03.2022	08.02.2022	Kernel/WebDispatcher (only Textupdate)

Example 3: Service Pack Aging

24 Month Rule for Security Notes (AS ABAP, AS JAVA)

Finding:

- Starting June 11, 2019, for all new SAP Security Notes with high or very high priority SAP delivers fix for Support Packages shipped within the last 24 months*. See <https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>
- Especially the ABAP Basis components and their age are critical because these components are usually affected by security patches.

Impact:

- Unpatched systems are prone for the misuse of vulnerabilities. Depending on the criticality of the patch it could lead to complete system compromise.

Recommendation:

- Bring the Service Pack age up to date and develop a SP patch plan especially for the critical components which are more affected from security flaws than others. See therefore the corresponding components like listed in the Patch advisory or system recommendation.
- Setup a SP age monitoring instance to detect and rate the SPs which are running out of the 24-month rule

Installed Software Component Versions					Installed Product Versions	
Component	Release	SP-Level	Support Package	Short Description of Component		
SAP_BASIS	751	0004	SAPK-75104INSAPBASIS	SAP Basis Component		
SAP_ABA	75B	0004	SAPK-75B04INSAPABA	Cross-Application Component		
SAP_GWFND	751	0004	SAPK-75104INSAPGWFND	SAP Gateway Foundation 7.40		
SAP_UI	752	0001	SAPK-75201INSAPUI	User Interface Technology		
ST-PI	740	0012	SAPK-74012INSTPI	SAP Solution Tools Plug-In		
SAP_BW	751	0004	SAPK-75104INSAPBW	SAP Business Warehouse		
UIBAS001	300	0000	-	UI for Basis Applications 1.0		
GRCPINW	V1100_731	0020	SAPK-11520INGRCPINW	SAP GRC NetWeaver Plug-In		
MDG_FND	801	0003	SAPK-80103INMDGFND	MDG Foundation		
WEBCUIF	801	0003	SAPK-80103INWEBCUIF	SAP Web UI Framework		
MDG_APPL	801	0003	SAPK-80103INMDGAPPL	MDG Applications		
MDG_UX	801	0003	SAPK-80103INMDGLUX	MDG Additional User Interface		

Component	Release	SP Level	Support-Package	Short Description of Component	Release Date	Age In Months
SAP_BASIS	751	0004	SAPK-75104INSAPBASIS	SAP Basis Component	05.10.17	29
SAP_ABA	75B	0004	SAPK-75B04INSAPABA	Cross-Application Component	05.10.17	29
SAP_GWFND	751	0004	SAPK-75104INSAPGWFND	SAP Gateway Foundation 7.40	05.10.17	29
SAP_UI	752	0001	SAPK-75201INSAPUI	User Interface Technology	11.09.17	29
ST-PI	740	0012	SAPK-74012INSTPI	SAP Solution Tools Plug-In	02.12.19	3
SAP_BW	751	0004	SAPK-75104INSAPBW	SAP Business Warehouse	05.10.17	29
UIBAS001	300	0000	-	UI for Basis Applications 1.0	11.09.17	29
GRCPINW	V1100_731	0020	SAPK-11520INGRCPINW	SAP GRC NetWeaver Plug-In	19.10.17	28
MDG_FND	801	0003	SAPK-80103INMDGFND	MDG Foundation	24.10.17	28
WEBCUIF	801	0003	SAPK-80103INWEBCUIF	SAP Web UI Framework	24.10.17	28
MDG_APPL	801	0003	SAPK-80103INMDGAPPL	MDG Applications	24.10.17	28
MDG_UX	801	0003	SAPK-80103INMDGLUX	MDG Additional User Interface	24.10.17	28
S4CORE	101	0003	SAPK-10103INS4CORE	S4CORE	24.10.17	28
SAP_HR	608	0045	SAPKE60845	Human Resources	14.09.17	29
SAP_HRCAE	608	0045	SAPK-60845INSAPHRCAE	Subcomponent SAP_HRCAE of SAP_HR	14.09.17	29
SAP_HRCAR	608	0045	SAPK-60845INSAPHRCAR	Subcomponent SAP_HRCAR of SAP_HR	14.09.17	29
SAP_HRCAT	608	0045	SAPK-60845INSAPHRCAT	Subcomponent SAP_HRCAT of SAP_HR	14.09.17	29
SAP_HRCAU	608	0045	SAPK-60845INSAPHRCAU	Subcomponent SAP_HRCAU of SAP_HR	14.09.17	29
SAP_HRCBE	608	0045	SAPK-60845INSAPHRCBE	Subcomponent SAP_HRCBE of SAP_HR	14.09.17	29
SAP_HRCBG	608	0045	SAPK-60845INSAPHRCBG	Subcomponent SAP_HRCBG of SAP_HR	14.09.17	29
SAP_HRCBR	608	0045	SAPK-60845INSAPHRCBR	Subcomponent SAP_HRCBR of SAP_HR	14.09.17	29
SAP_HRCCA	608	0045	SAPK-60845INSAPHRCCA	Subcomponent SAP_HRCCA of SAP_HR	14.09.17	29
SAP_HRCCH	608	0045	SAPK-60845INSAPHRCCH	Subcomponent SAP_HRCCH of SAP_HR	14.09.17	29
SAP_HRCCL	608	0045	SAPK-60845INSAPHRCCL	Subcomponent SAP_HRCCL of SAP_HR	14.09.17	29
SAP_HRCCL	608	0045	SAPK-60845INSAPHRCCN	Subcomponent SAP_HRCCL of SAP_HR	14.09.17	29
SAP_HRCCL	608	0045	SAPK-60845INSAPHRCCN	Subcomponent SAP_HRCCL of SAP_HR	14.09.17	29
SAP_HRCCL	608	0045	SAPK-60845INSAPHRCCO	Subcomponent SAP_HRCCL of SAP_HR	14.09.17	29
SAP_HRCCL	608	0045	SAPK-60845INSAPHRCCZ	Subcomponent SAP_HRCCL of SAP_HR	14.09.17	29
SAP_HRCDE	608	0045	SAPK-60845INSAPHRCDE	Subcomponent SAP_HRCDE of SAP_HR	14.09.17	29
SAP_HRCDE	608	0045	SAPK-60845INSAPHRCDK	Subcomponent SAP_HRCDE of SAP_HR	14.09.17	29
SAP_HRCDE	608	0045	SAPK-60845INSAPHRCEG	Subcomponent SAP_HRCDE of SAP_HR	14.09.17	29
SAP_HRCES	608	0045	SAPK-60845INSAPHRCES	Subcomponent SAP_HRCES of SAP_HR	14.09.17	29
SAP_HRCFI	608	0045	SAPK-60845INSAPHRCFI	Subcomponent SAP_HRCFI of SAP_HR	14.09.17	29
SAP_HRCFR	608	0045	SAPK-60845INSAPHRCFR	Subcomponent SAP_HRCFR of SAP_HR	14.09.17	29
SAP_HRCGB	608	0045	SAPK-60845INSAPHRCGB	Subcomponent SAP_HRCGB of SAP_HR	14.09.17	29

Validation of the Age of Support Package

based on SP Release-to-Customer date of any Software Component known in SAP PPMS***

SAP Configuration & Security Analytics

Validation

*Policy: Age of component level 3.0 FP01

Validated at 17.11.2021, 13:26:30 - 5 hours ago

Systems

0.0% Compliance
100.0%

Check Items

0.0% Compliance
100.0%

Systems / Checks

0.0% Compliance
100.0%

Systems Checks Systems / Checks

Compliance of systems

Technical Systems - Items: 5

Compliant	Customer	System ID	System Type	% Non Compliant	# Non Compliant	# Compliant	IT Admin Role	Lifecycle Status
<input checked="" type="checkbox"/> Yes	DLM	MT8DLM	Application Server Java	<input type="text" value="0"/>	0	66	Undefined	Active
<input checked="" type="checkbox"/> Yes	DLM	N72DLM	Application Server Java	<input type="text" value="0"/>	0	133	Demo System	Active
<input checked="" type="checkbox"/> Yes	SSC	FQJSSC	Application Server Java	<input type="text" value="0"/>	0	69	Production System	Active
<input checked="" type="checkbox"/> Yes	Tyrell Motors	JC5TMO	Application Server Java	<input type="text" value="0"/>	0	66	Undefined	Active
<input checked="" type="checkbox"/> Yes	Tyrell Motors	JC6TMO	Application Server Java	<input type="text" value="0"/>	0	66	Undefined	Active

***currently an issue with SP00

Age of Support Package Validation

Just a few lines of xml code – applicable to all AS ABAP and AS JAVA Software Components

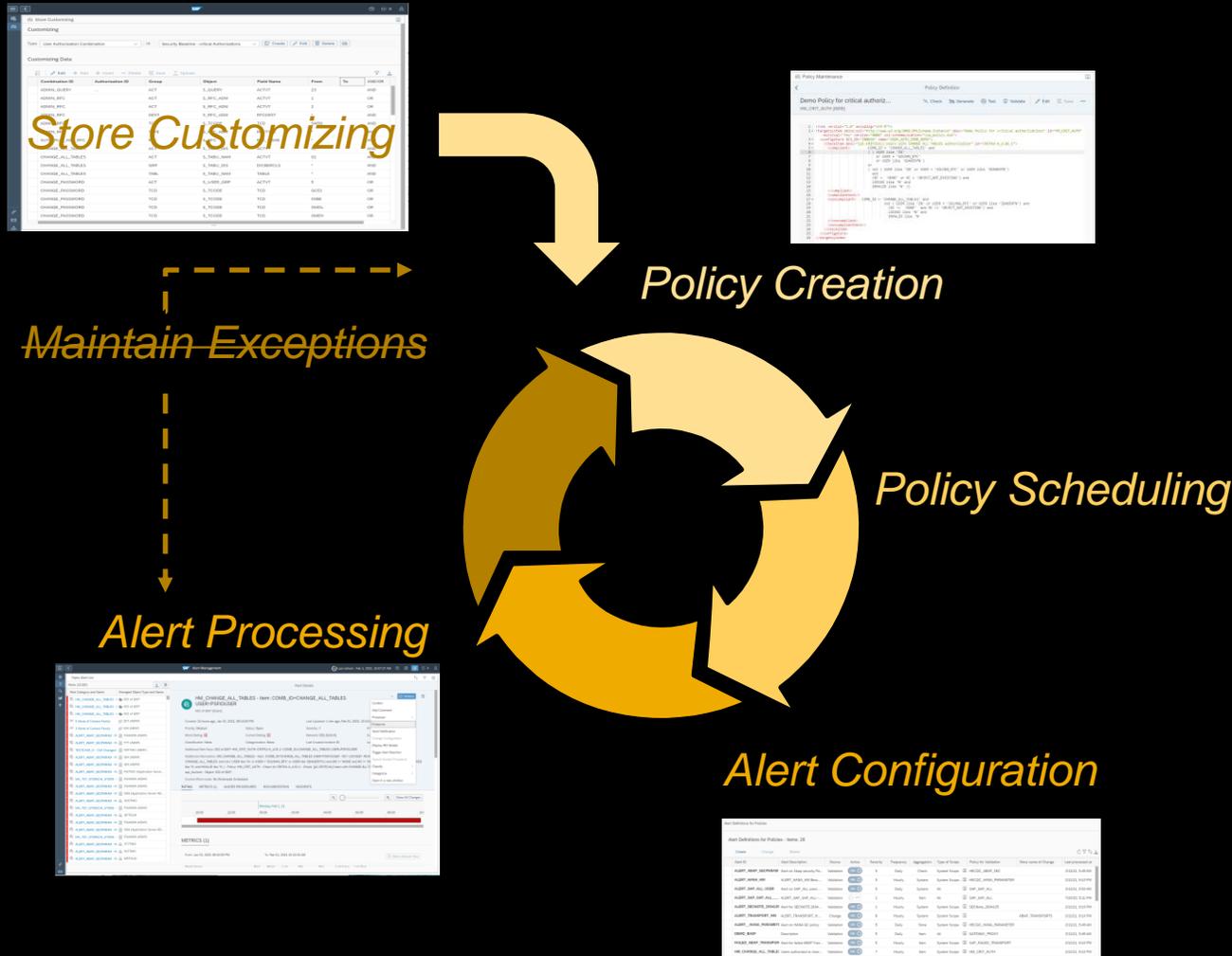
The screenshot shows a GitHub repository page for 'SAP-samples / frun-csa-policies-best-practices'. The file tree on the left shows a folder named 'FRUN3.0 FP01 AgeOfComponents' highlighted with a green box. A green arrow points from this folder to the XML code snippet on the right. The XML code is a SAP TargetSystem configuration for validating the age of software components.

```
1 <?xml version="1.0" encoding="utf-8"?>
2
3 <!--
4 Exclude software components for which SP_REL_DATE is empty
5 Version: 002
6 Date: July 16 2021
7 -->
8 <targetsystem xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" desc="Age of component level 3.0 FP01" id="AGE_OF_COMP_LEVEL" multisql="Yes" version="0000" xsi:schemaLocat
9 <!-- Basic -->
10 <configstore name="COMP_LEVEL">
11 <checkitem desc="Age of Component Level - ABAP" id="ABAP.AGE_COMP.01" not_found="ignore" system_attributes="SYSTEM_TYPE:ABAP">
12 <compliant>
13 COMPONENT like '%' and VERSION like '%' and SP_REL_DATE != '' and (add_days(current_date,-730)) &lt; (CASE WHEN SP_REL_DATE like_regexpr '^d{8,8}$' THEN SP_REL_DATE WHE
14 </compliant>
15 <noncompliant>
16 COMPONENT like '%' and VERSION like '%' and SP_REL_DATE != '' and not (add_days(current_date,-730)) &lt; (CASE WHEN SP_REL_DATE like_regexpr '^d{8,8}$' THEN SP_REL_DATE
17 </noncompliant>
18 </checkitem>
19 <checkitem desc="Age of Component Level - JAVA" id="JAVA.AGE_COMP.01" not_found="ignore" system_attributes="SYSTEM_TYPE:JAVA">
20 <compliant>
21 COMPONENT like '%' and VERSION like '%' and SP_REL_DATE != '' and (add_days(current_date,-730)) &lt; (CASE WHEN SP_REL_DATE like_regexpr '^d{8,8}$' THEN SP_REL_DATE WHEN
22 </compliant>
23 <noncompliant>
24 COMPONENT like '%' and VERSION like '%' and SP_REL_DATE != '' and not (add_days(current_date,-730)) &lt; (CASE WHEN SP_REL_DATE like_regexpr '^d{8,8}$' THEN SP_REL_DATE
25 </noncompliant>
26 </checkitem>
27 </configstore>
28 </targetsystem>
```

Adoption Journey – Users & Authorizations

Get Clean Projects – Users*** and Authorizations

Data on Users, Authorizations and Roles is available only after store customizing



Focused Run – Immediate Benefits:

- ✓ Templates of customizable data collectors
- ✓ ABAP Profiles
- ✓ Role and User relation
- ✓ Role Authorization Combination
- ✓ Role by pattern
- ✓ Sensitive Table Access by Role
- ✓ Sensitive Transaction Access by Role
- ✓ User Authorization Combination
- ✓ User Types
- ✓ ABAP: Name / Value Store by function module
- ✓ HANA: NAME / VALUE Store from database by SQL
- ✓ HANA Granted Privileges
- ✓ HANA Granted Roles
- ✓ Mostly equivalent to Solution Manager (some enhancements)
- ✓ For critical privileges, you can directly create alerts from CSA (flexible severity and aggregation – even on item-level)

User Configuration in RFC Destinations (Requirement: User Type = System)

1. Identify RFC Destinations with user names
(e.g. if exist: compliant naming convention)
2. Validate users, e.g.:
 - a. Type for users is compliant to naming convention
 - b. User name is in list of users of type System

Limited capabilities for validation of users and authorizations.

May complement Access Control systems for users that are part of technical configurations.

Store Customizing

Customizing

Type: Id:

Customizing Data

Check ID	User Name	User Type
RFC_USER	RFC*	*
TYPE_SYSTEM	*	SYSTEM

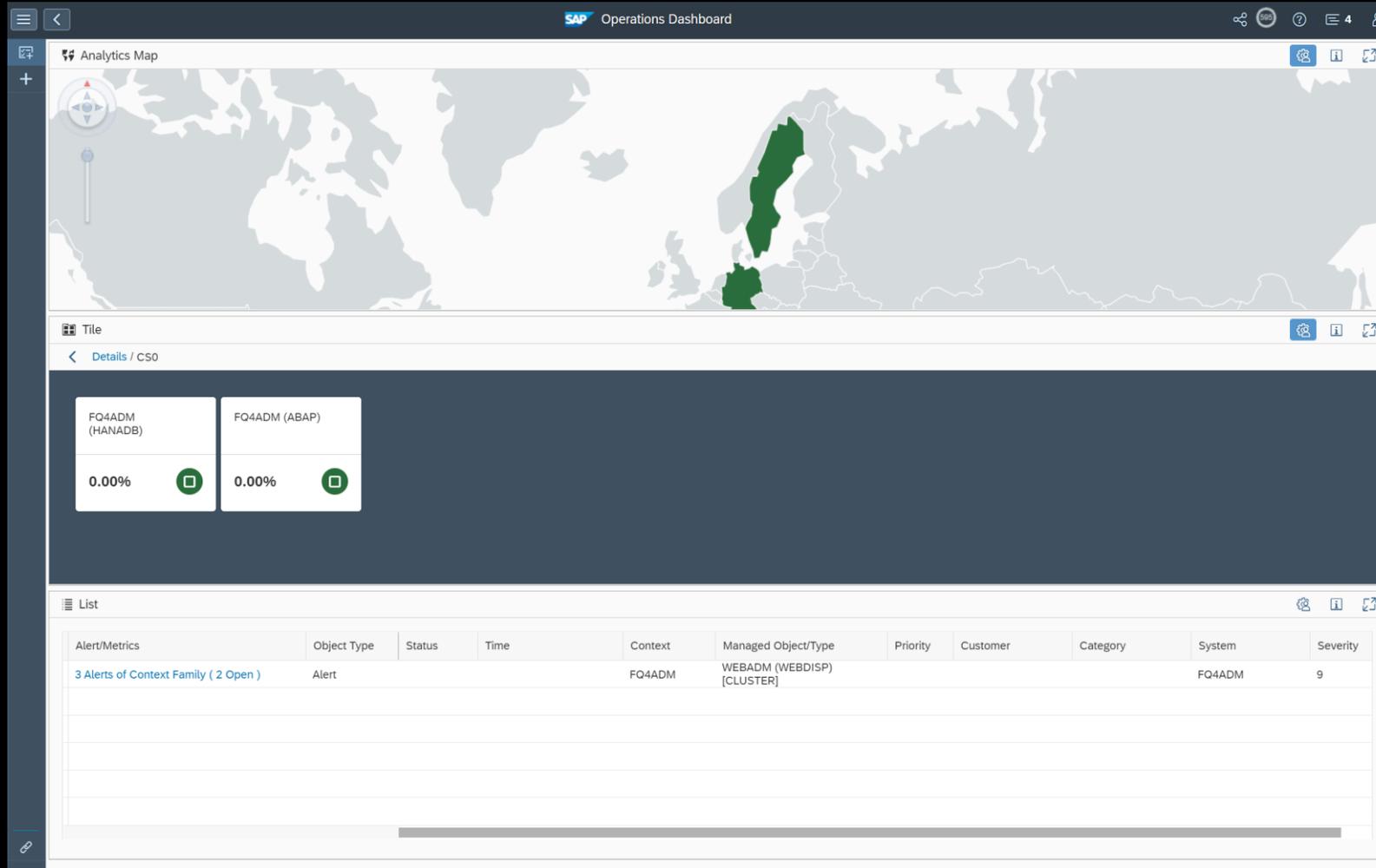
User Types for RFC (RFC_USER_TYPE_INFO) - Items: 51 - displayed: 51

ConfigItemKey	Value	Type of event	Valid since
CHECK_ID = RFC_USER USER =	USER_TYPE = USER_GROUP = USER_LOCKED = USER_INVALID =	INITIAL	11/14/21, 5:19 PM
CHECK_ID = TYPE_SYSTEM USER = FRN_AIM_ADM	USER_TYPE = SYSTEM USER_GROUP = USER_LOCKED = FALSE USER_INVALID = FALSE	INITIAL	11/14/21, 5:19 PM
CHECK_ID = TYPE_SYSTEM USER = FRN_AIM_ETD	USER_TYPE = SYSTEM USER_GROUP = USER_LOCKED = FALSE USER_INVALID = FALSE	INITIAL	11/14/21, 5:19 PM
CHECK_ID = TYPE_SYSTEM USER = FRN_AJM_ADM	USER_TYPE = SYSTEM USER_GROUP = USER_LOCKED = FALSE USER_INVALID = FALSE	INITIAL	11/14/21, 5:19 PM
CHECK_ID = TYPE_SYSTEM USER = FRN_AJM_ETD	USER_TYPE = SYSTEM USER_GROUP = USER_LOCKED = FALSE USER_INVALID = FALSE	INITIAL	11/14/21, 5:19 PM

Adoption Journey – Dashboard

Operation Dashboard – Example

CSA Alerts included as of FRUN 3.0 FP02



Monitor Alerts (or Metrics) that are critical to Operations

(including Security Configurations)

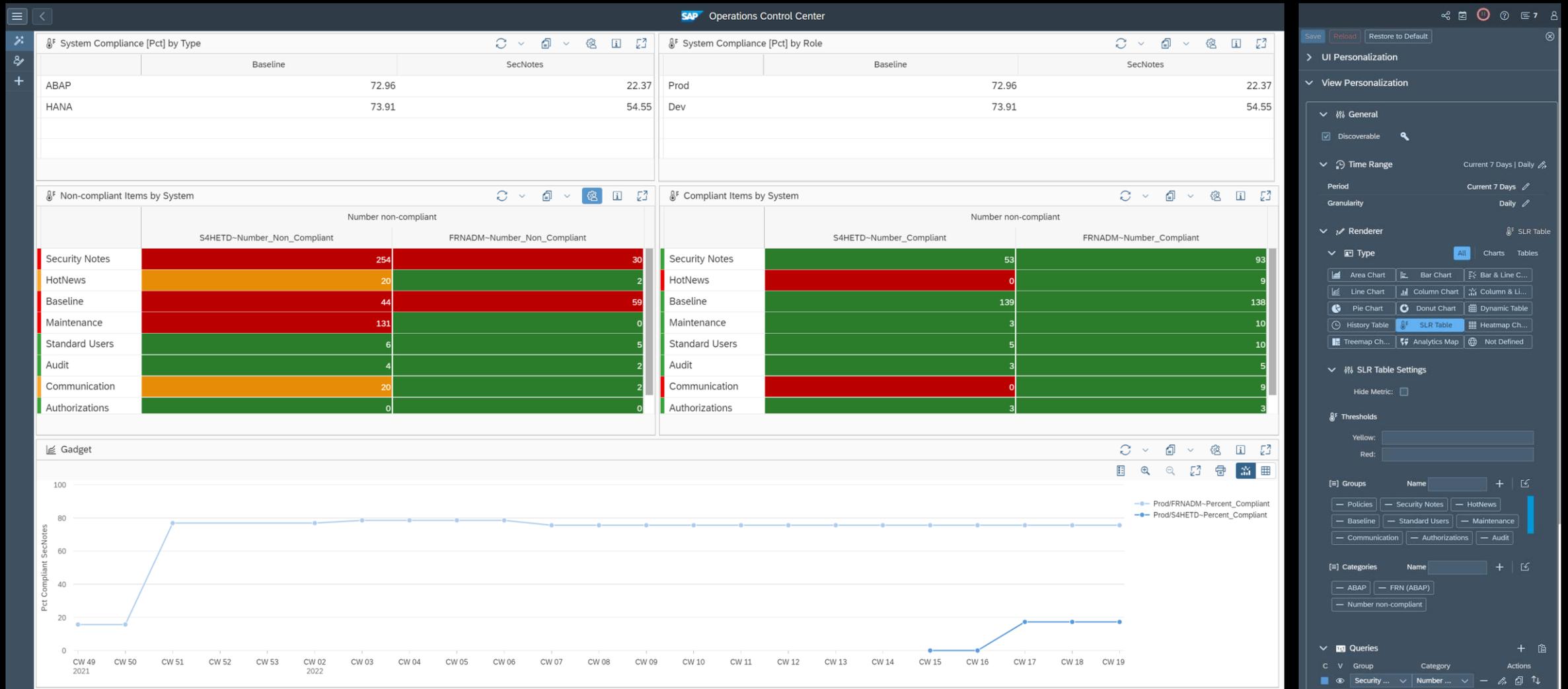
Predefined Page Structure:

- Map
- Tiles w/ Drill-down
- Alert Ticker

Filter by Alert Category and Severity

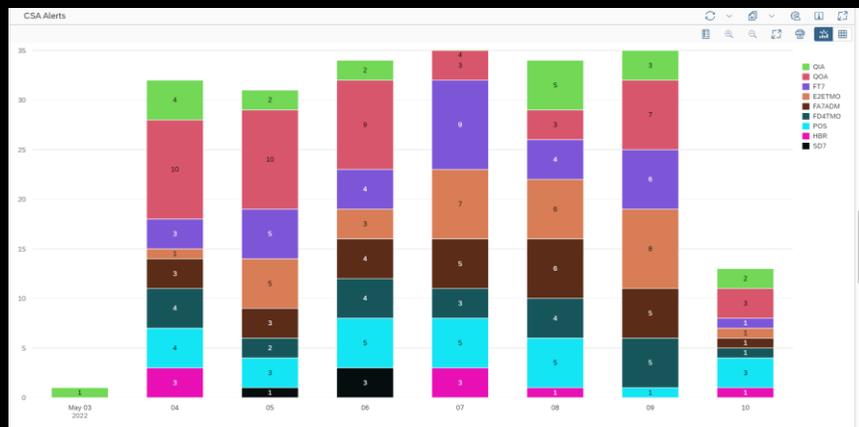
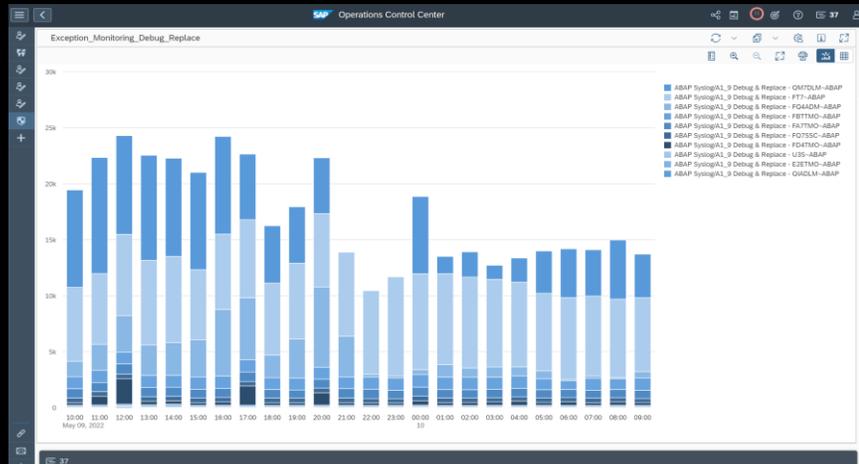
[Operations Dashboard \(sap.corp\)](https://sap.com)

OCC Dashboard – Example



OCC Dashboard –Example

Operations Control Center (sap.corp)



CSA Policies	R21	Y13	CCF	E2ETMO	E73	FA7TMO	FBTTMO	FD4TMO	FQ4ADM	FQ755C	FT7	HAD	HBR	HHATMO	POS
RFC Connectivity			66.7	66.7	0.0	81.0	100.0	66.7	66.7	66.7	66.7	66.7	66.7	66.7	66.7
Web Dispatcher Secu				75.0	100.0	75.0	50.0	50.0	50.0	50.0	75.0	50.0	50.0	50.0	50.0
ABAP Default Users H				22.7	35.7	22.7	25.0	27.8	35.7	14.3	21.4	36.4	2.3	35.7	
Users with Critical Pr				93.9	88.9	98.9	99.2	99.4	99.4	98.0	98.0	99.3	99.8	95.9	
Security Audit Log				100.0	100.0	100.0	0.0	0.0	66.7	100.0	100.0	0.0	0.0	100.0	
Profile Parameters				63.6	81.8	59.1	45.5	45.5	40.9	54.5	45.5	45.5	27.3	63.6	
ABAP Instance Param				65.2	82.6	60.9	47.8	47.8	43.5	56.5	47.8	47.8	30.4	65.2	
Password Hashes				85.7	37.5	9.1	0.0	31.3	26.1	0.0	11.1	64.7	35.7	37.5	
Open Clients				0.0	25.0	0.0	0.0	0.0	25.0	0.0	25.0	0.0	0.0	0.0	
RFC Gateway	33.3	100.0	10.4	50.0	40.0	1.8	3.2	6.3	0.0	1.8	3.3	0.0	2.9	16.7	
Message Server Secu	100.0			33.3	40.0	0.0	0.0	14.3	25.0	0.0	0.0	25.0	14.3	25.0	
Limit SICF Content				0.0	0.0	56.3	56.3	6.3	0.0	6.3	0.0	0.0	6.3	12.5	
Java UME Parameter:															
Secure Java Configur															
SAP HANA Security															



Exceptions
(Debug/Replace events)

CSA Policies
(Baseline Compliance per Topic)

CSA Alerts
(stacked by System)

CSA Policies
(Baseline Compliance per System)

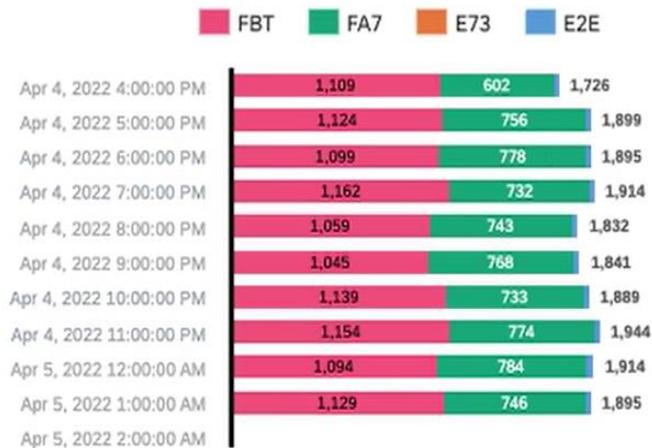


This XML file does not appear to have any style information associated with it. The document tree is shown below.

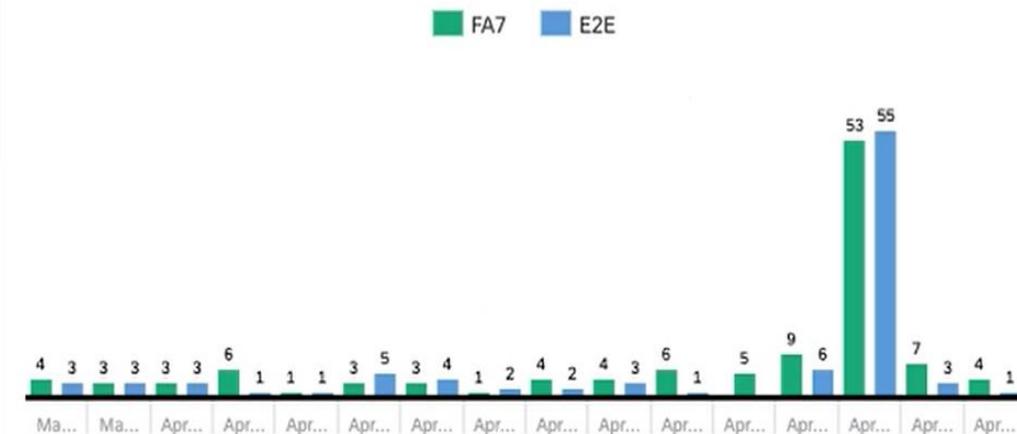
```
<?xml version="1.0" encoding="utf-8" ?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices"
xml:base="https://FRUN.ALMDemo.COM:443/sap/opu/odata/sap/frn_fi_dp_srv/">
  <id>https://FRUN.ALMDemo.COM:443/sap/opu/odata/sap/frn_fi_dp_srv/SeriesSacSet</id>
  <title type="text">SeriesSacSet</title>
  <updated>2022-05-09T16:01:12Z</updated>
  <author>
    <name/>
  </author>
  <link href="SeriesSacSet" rel="self" title="SeriesSacSet"/>
  <entry>
    <id>https://FRUN.ALMDemo.COM:443/sap/opu/odata/sap/frn_fi_dp_srv/SeriesSacSet(IdDashboard='0AB3AC7C85C51EECA2E372EA62A0B615',IdGadget='guid_b60e625b-07f6-4902-a5fe-26982a44bfbe')</id>
    <title type="text">SeriesSacSet(IdDashboard='0AB3AC7C85C51EECA2E372EA62A0B615',IdGadget='guid_b60e625b-07f6-4902-a5fe-26982a44bfbe')</title>
    <updated>2022-05-09T16:01:12Z</updated>
    <category term="FRN_FI_DP_SRV.SeriesSac" scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme"/>
    <link href="SeriesSacSet(IdDashboard='0AB3AC7C85C51EECA2E372EA62A0B615',IdGadget='guid_b60e625b-07f6-4902-a5fe-26982a44bfbe')" rel="self" title="SeriesSac"/>
    <content type="application/xml">
      <m:properties xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices">
        <d:IdDashboard>0AB3AC7C85C51EECA2E372EA62A0B615</d:IdDashboard>
        <d:IdGadget>guid_b60e625b-07f6-4902-a5fe-26982a44bfbe</d:IdGadget>
        <d:DashboardName>SAP Baseline (Number Noncompliances)</d:DashboardName>
        <d:GadgetName>Non-compliant Items by System</d:GadgetName>
        <d:Name>Number non-compliant-S4HETD~Number_Non_Compliant</d:Name>
        <d:QueryNumber>1 </d:QueryNumber>
        <d:GROUP>Security Notes</d:GROUP>
        <d:G2Y>20</d:G2Y>
        <d:Y2R>30</d:Y2R>
        <d:TREND>DOWN</d:TREND>
        <d:METHOD/>
        <d:SOURCE>DP_CSA</d:SOURCE>
        <d:RESOLUTION>DAY</d:RESOLUTION>
        <d:VALUE>254.00</d:VALUE>
        <d:TIMESTAMP>20220503000000</d:TIMESTAMP>
        <d:DATE>20220503</d:DATE>
        <d:WEEK>202218</d:WEEK>
        <d:WEEKDAY>2</d:WEEKDAY>
        <d:HOURL>00</d:HOURL>
        <d:DIMENSION1>NO_PD_ABAP</d:DIMENSION1>
        <d:DIMENSION2>Number_Non_Compliant</d:DIMENSION2>
        <d:DIMENSION3>S4HETD</d:DIMENSION3>
        <d:DIMENSION4>ABAP</d:DIMENSION4>
        <d:DIMENSION5/>
        <d:DIMENSION6>0AB3AC7C85C51EECA3FB881157BCD615</d:DIMENSION6>
      </m:properties>
    </content>
  </entry>
  <entry>
    <id>https://FRUN.ALMDemo.COM:443/sap/opu/odata/sap/frn_fi_dp_srv/SeriesSacSet(IdDashboard='0AB3AC7C85C51EECA2E372EA62A0B615',IdGadget='guid_b60e625b-07f6-4902-a5fe-26982a44bfbe')</id>
    <title type="text">SeriesSacSet(IdDashboard='0AB3AC7C85C51EECA2E372EA62A0B615',IdGadget='guid_b60e625b-07f6-4902-a5fe-26982a44bfbe')</title>
    <updated>2022-05-09T16:01:12Z</updated>
    <category term="FRN_FI_DP_SRV.SeriesSac" scheme="http://schemas.microsoft.com/ado/2007/08/dataservices/scheme"/>
    <link href="SeriesSacSet(IdDashboard='0AB3AC7C85C51EECA2E372EA62A0B615',IdGadget='guid_b60e625b-07f6-4902-a5fe-26982a44bfbe')" rel="self" title="SeriesSac"/>
    <content type="application/xml">
      <m:properties xmlns:m="http://schemas.microsoft.com/ado/2007/08/dataservices/metadata" xmlns:d="http://schemas.microsoft.com/ado/2007/08/dataservices">
        <d:IdDashboard>0AB3AC7C85C51EECA2E372EA62A0B615</d:IdDashboard>
```

Debug & Replace Activities per system

1 Filter



Configuration & Security Analysis Alerts



SID

All

E2E

E73

FA7

FBT

FD4

FQ4

FQ7

Total Number of Security Alerts

234

Alerts

Overall Compliancy %

46.91

% Non Compliant

53.09

% Compliant

% of Non Compliant Items per Policy (ABAP)

1 Filter | 2 Explorer Views

ABAP Default Users Handling	22.73	35.71	22.73	25.00
ABAP Instance Parameter	65.22	82.61	60.87	47.83
Limit SICF Content	0.00	0.00	56.25	56.25
Message Server Security	33.33	40.00	0.00	0.00
Open Clients	0.00	25.00	0.00	0.00
Password Hashes	85.71	37.50	9.09	0.00
Profile Parameters	63.64	81.82	59.09	45.45
RFC Connectivity	66.67	0.00	100.00	100.00
RFC Gateway	50.00	40.00	1.79	3.23
Security Audit Log	100.00	100.00	100.00	0.00
Users with Critical Profiles	93.94	88.89	98.90	99.24
Web Dispatcher Security	75.00	100.00	75.00	50.00
	E2E	E73	FA7	FBT



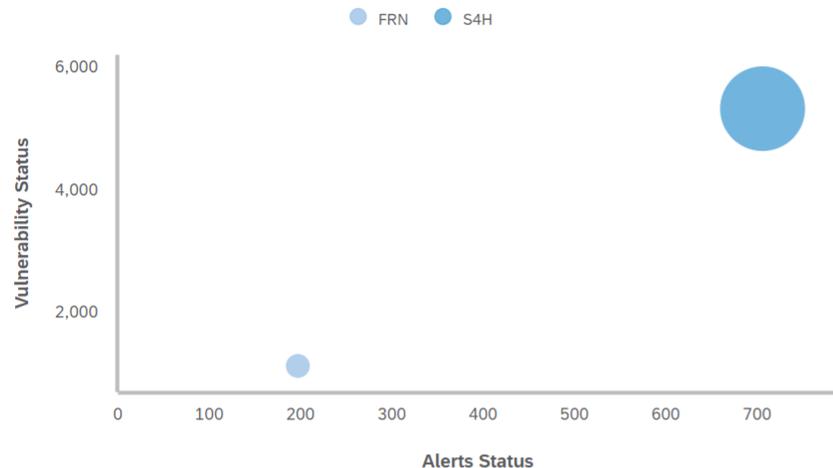
Overall Security Status by System

System ID

- All
- FRN
- S4H

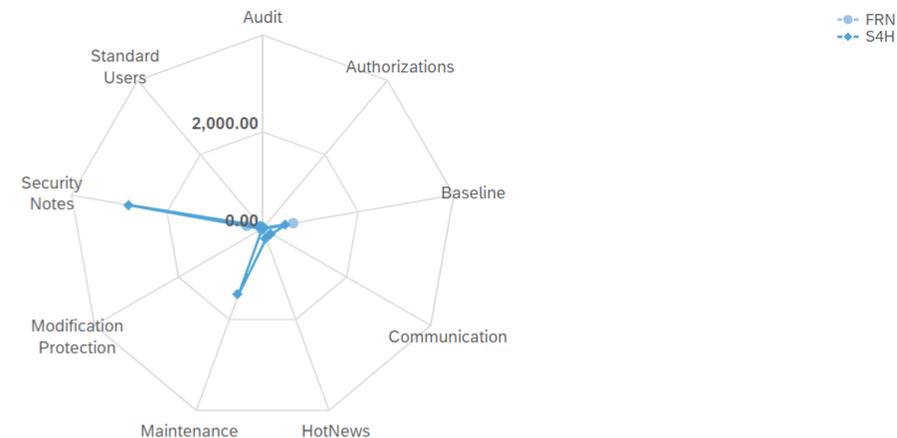
Systems Status

Explorer Available



Count per Category, System

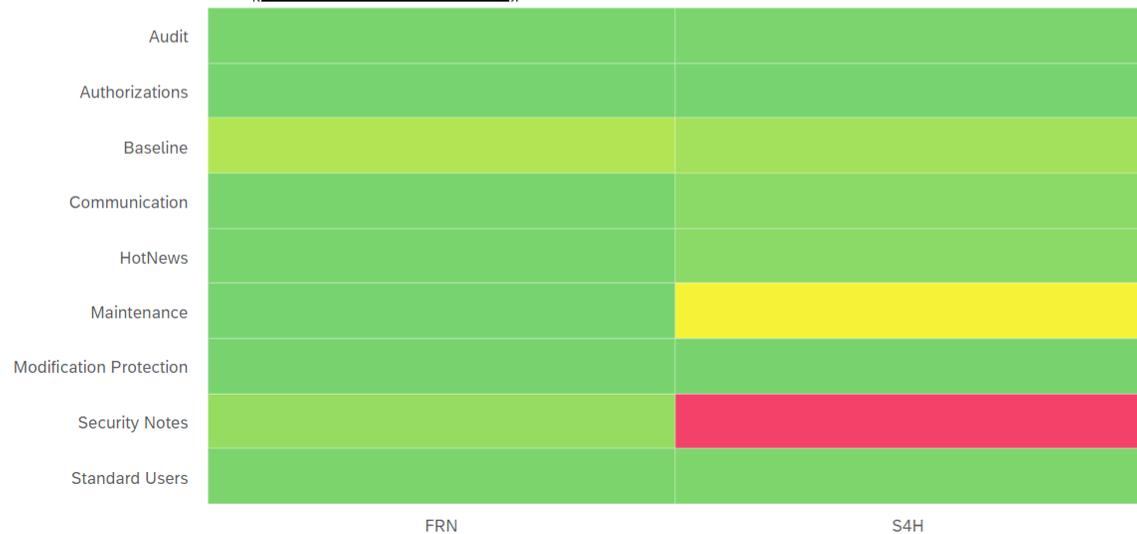
Explorer Available



Vulnerability Status per Policy, System

Explorer Available

(Initiate Remediation Action)



Alerts Overview

MainSystemId	Alert Name	FRUN Category	Severity	Status	Measures	Alert Score
					Alert Date	
(Null)	Low Log Amount per system	Baseline	MEDIUM	OPEN	Mar 30, 2022	100
					Mar 31, 2022	100
					Apr 1, 2022	100
					Apr 5, 2022	100
					Apr 6, 2022	100
					Apr 8, 2022	100
					Apr 12, 2022	100
					Apr 13, 2022	100
					Apr 15, 2022	100
					Apr 19, 2022	100
					Apr 20, 2022	100
					Apr 21, 2022	100
					Apr 26, 2022	100
					Apr 27, 2022	100
					Apr 28, 2022	100
					Apr 28, 2022	100
					Apr 29, 2022	100
\$T1	Authorization assignment by non-admin-group ...	Baseline	HIGH	OPEN	Mar 29, 2022	12,900
					Mar 30, 2022	19,800
					Mar 31, 2022	18,000

SAP Focused Run for Configuration & Security Summary

Create and adapt validation policies based on

- SAP Best Practice and latest vendor expertise
- Custom-specific governance rules
- Custom-specific improvement focus
- Ad-hoc requirements

Report on

- Actual Deployment Status
- Actual Management Status (including grace periods, process SLA, accepted risk)

Report into

- Standard Processes
- Central Infrastructures

```

BL_5-6 [0000] | SAP BASELINE BL_5-6 (RFC CONNECTIVITY)
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!-- targetsystem desc="RFC Connectivity" id="BL_5-6" multiql="Yes" -->
3 <!-- configid name="ABAP_INSTANCE_PARAM" -->
4 <!-- checkid desc="Transaction option for the RFC authority check" id="BL_5-6-01" -->
5 <!-- compliantNAME = 'auth/rfc_authority_check' and VALUE = '1' --> </compliant -->
6 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
7 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
8 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
9 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
10 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
11 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
12 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
13 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
14 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
15 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
16 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
17 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
18 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
19 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
20 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
21 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
22 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
23 <!-- compliantNAME = 'auth/rfc_authority_check' and not ( VALUE = '1' ) --> </noncompliant -->
    
```

Policy Maintenance



Search & Browse

Item	Item Name	Compliance	Status
Software component	COMP_LEVEL	COMPONENT + SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0
Software component	COMP_LEVEL	COMPONENT + SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0
Software component	COMP_LEVEL	COMPONENT + SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0
Software component	COMP_LEVEL	COMPONENT + SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0

Validation

Validation



Exemptions

Item	Item Name	Compliance	Status
SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0
SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0
SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0
SAP_BASIS	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0	VERSION + T10 SP + 010 PATCH + 0

Exemptions

Dashboard

Dashboard

Alert Inbox

Alert	Severity	Category	Created	Resolved
System Health Check	High	Configuration	2018-10-26 10:00:00	2018-10-26 10:00:00
System Health Check	Medium	Configuration	2018-10-26 10:00:00	2018-10-26 10:00:00
System Health Check	Low	Configuration	2018-10-26 10:00:00	2018-10-26 10:00:00

Alert Inbox

Report

Report



**Thank
You!**

Thank you.

Contact information:

Dr. Hendrik Mueller

SAP SE

hendrik.mueller@sap.com

Follow us



www.sap.com/contactsap

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/trademark for additional trademark information and notices.

SAP folgen auf



www.sap.com/germany/contactsap

© 2021 SAP SE oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere sind die SAP SE oder ihre Konzernunternehmen in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen. Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen der SAP SE oder ihrer Konzernunternehmen können von der SAP SE oder ihren Konzernunternehmen jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.

SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite www.sap.com/trademark