How to minimize the attack surface of hybrid SAP landscapes?

Dr. Hendrik Mueller, SAP SE
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

Risk Management

Process Control

Access Control

Inventory & Maintenance

Configurations

Authorizations & SoD

Custom Code

Events & Log Patterns

Compliance

Security Dashboard
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**

- Integration Monitoring (AIM)
- User Monitoring (AUM)
- Application Management (AAM)
- Configuration Monitoring (ACM)
- System Management (ASM)
- Event & Alert Management (AEM)
- Root Cause Analysis (ARA)
- Analytics & Intelligence (AAI)

**Technology Foundation:** SAP HANA / SAP NetWeaver ABAP + SAPUI5

Embedded into comprehensive set of IT Operations Use Cases
From ... data ... to ... validation ... to ... dashboard

Scheduled Data Collection

Config Stores & Change History

Scheduled Policies & Alerts

Dashboard Pages

API

HANA System(s)

System (ABAP)

System (JAVA)

Collector Inbound Queue

Configuration and Change Database

CCDB_DATA_001

CCDB_DATA_XXX

CCDB

FRUN2SAC
Customer Journey to Security with SAP Focused Run

- **Stay ahead**
  - track security improvements
  - analyze latest threats
  - analyze prerequisites of planned security measures

- **Keep running**
  - react on HotNews
  - monitor expiring certificates, mandatory transports, ...

- **Stay clean**
  - new SAP Security Notes
  - timely transparency → report vulnerability and deployment
  - automate operational processes

- **Get clean**
  - SAP Security Baseline Template
  - detect & analyze → define/automate security baseline → validate and verify

- **Custom Policies**
- **SAP or Custom Policies**
- **PatchDay Policies** (monthly)
- **Baseline Policies** (250+ Checks)
- **SAP Github Content**
- **Focused Run UI**
Adoption Journey – SAP Baseline
Prevent Breaches with a strong Security Baseline
Keep doors and widows 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

User & Identity Management
- SAP Standard User

Authentication & Single Sign-On
- Password Policy
- SAP Logon Tickets
- Password Hashes

Roles & Authorizations
- Switchable Authorization Checks
- Profile Parameter & Customizing
- Critical Authorizations

Security Monitoring & Forensics
- Process
- Logging Content
- Profile Parameters

Security Hardening: General
- Other Profile Parameters
- Modification Protection
- ABAP Standard User
- Security Store
- Directory Traversal
- Security Audit Log

Security Hardening: Communication Security
- RFC Connectivity
- RFC Profile Parameter
- RFC Trusted System Security
- RFC Gateway Security
- Securing RFC / DIAG
- RFC Callback
- RFC UCON

Security Hardening: Web Access
- 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
- SAPStartSrv
- SAP Host Agent
- Message Server Security
- Enqueue Server

User & Identity Management
- SAP Standard User

Authentication & Single Sign-On
- Password Policy
- SAP Logon Tickets
- Password Hashes

Roles & Authorizations
- Switchable Authorization Checks
- Profile Parameter & Customizing
- Critical Authorizations

Security Monitoring & Forensics
- Process
- Logging Content
- Profile Parameters

Security Hardening: General
- Other Profile Parameters
- Modification Protection
- ABAP Standard User
- Security Store
- Directory Traversal
- Security Audit Log

Security Hardening: Communication Security
- RFC Connectivity
- RFC Profile Parameter
- RFC Trusted System Security
- RFC Gateway Security
- Securing RFC / DIAG
- RFC Callback
- RFC UCON

Security Hardening: Web Access
- 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
- SAPStartSrv
- SAP Host Agent
- Message Server Security
- Enqueue Server

© 2021 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
SAP Security Baseline Template: (SAP Note: 2253549)
Specific Technical Rules on a Detail Level

1 Overview, Requirements and Guidelines ............................................... 10
2 Regulations .................................................................................................. 10
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) .......................................................... 18
2.2.1 Secure Maintenance of SAP Code .................................................. 18
2.2.2 Custom Code Security ................................................................. 18
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
3.2 Annotations and Additional Information ............................................. 28
3.3 Infrastructure Security ......................................................................... 30
3.3.1 Network Security ....................................................................... 30
3.3.1.1 Network Zones and Firewalls ................................................. 30
3.3.1.1.1 Client – Server Communication – ABAP Systems ........ 31
3.3.1.1.2 Client – Server Communication – Java Systems ............. 33
3.3.1.1.3 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
4.1.2.1 Operating System Support ..................................................... 38
4.1.2.1.1 Windows ........................................................................ 38
4.1.2.1.1.1 Windows Groups and Users in an SAP System Environment .................................................. 38
4.1.2.1.1.2 Windows Operating System User Settings in an SAP System .................................................. 38
4.1.2.1.1.3 SAP Systems in the Windows Domain Concept ........... 39
4.1.2.1.1.4 Securing Data Relevant to the SAP System .................. 39
4.1.2.1.1.5 Security Settings for Shared Memory .............................. 40
4.1.2.1.2 Unix .............................................................................. 40
4.1.2.1.2.1 Protecting Specific Properties, Files and Services .......... 40
4.1.2.1.2.2 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 Authorization and Encryption ......................................... 42
4.1.3.2 SAP-HANA Security ............................................................. 42
4.1.3.2.1 Change Passwords of Users after Handover ..................... 43
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 privilege 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 Login Attempts .................................................. 45
4.1.3.3.3 Use Secure Authentication ........................................... 45
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

The structure of the template is based on the SAP Secure Configuration Map:

SAP Security Baseline Template

Last update: 11/2021
Example 1: SE06 – Change Options (Configuration)
Example 1: SE06 – Change Options (Change Log)
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
Views on Validation and Trend Analysis
Create Alerts from Policies and Store Changes

Examples
CSA Alert Processing
Alert provides a link to CSA Validation Result for further details
Adoption Journey – SAP Security Notes
Example 2: SAP Security Notes Validation
After each SAP PatchDay

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

ABAP / HANA from GitHub (SAP-Samples)
## Security Notes (High, Hotnews) – Coverage with SAP Focused Run

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

#### May '22

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>CVSS Sc</th>
<th>CVSS Vi</th>
<th>Priority</th>
<th>Released</th>
<th>First Released</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2998510</td>
<td>[CVE-2022-28214] Central Management Server Information Discrepancy</td>
<td>7.8</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>10.05.22</td>
<td>10.05.22</td>
<td>BOBI Platform</td>
</tr>
<tr>
<td>3189409</td>
<td>[CVE-2022-22965] Remote Code Execution vulnerability associaci</td>
<td>9.8</td>
<td>CVSS:3.0</td>
<td>HotNews</td>
<td>10.05.22</td>
<td>10.05.22</td>
<td>Business One</td>
</tr>
<tr>
<td>3140046</td>
<td>[CVE-2022-27656] Cross-Site Scripting (XSS) vulnerability in adm</td>
<td>8.3</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>10.05.22</td>
<td>10.05.22</td>
<td>Webdispatcher, ABAP, JAVA</td>
</tr>
</tbody>
</table>

#### April '22

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>CVSS Sc</th>
<th>CVSS Vi</th>
<th>Priority</th>
<th>Released</th>
<th>First Released</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3158613</td>
<td>Update 1 to Security Note 3022622 - [CVE-2021-21480] Code in</td>
<td>9.1</td>
<td>CVSS:3.0</td>
<td>HotNews</td>
<td>12.04.22</td>
<td>12.04.22</td>
<td>JAVA</td>
</tr>
<tr>
<td>3155609</td>
<td>Privilege escalation vulnerability in Apache Tomcat server comj</td>
<td>7</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>12.04.22</td>
<td>12.04.22</td>
<td>Hybris Commerce</td>
</tr>
<tr>
<td>3130497</td>
<td>[CVE-2022-27671] CSRF token visible in one of the URL in SAP B</td>
<td>8.2</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>12.04.22</td>
<td>12.04.22</td>
<td>BO BI Platform</td>
</tr>
<tr>
<td>3111311</td>
<td>[CVE-2022-28772] Denial of service (DOS) in SAP Web Dispatcher</td>
<td>7.5</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>12.04.22</td>
<td>12.04.22</td>
<td>Kernel, WebD, XSA, XSC</td>
</tr>
<tr>
<td>3022622</td>
<td>[CVE-2021-21480] Code injection vulnerability in SAP Manufakt</td>
<td>9.1</td>
<td>CVSS:3.0</td>
<td>HotNews</td>
<td>12.04.22</td>
<td>09.03.2021</td>
<td>JAVA</td>
</tr>
<tr>
<td>3123936</td>
<td>[CVE-2022-22536] Request smuggling and request concatenatic</td>
<td>10</td>
<td>CVSS:3.0</td>
<td>HotNews</td>
<td>22.03.22</td>
<td>08.02.2022</td>
<td>Kernel, WebD</td>
</tr>
<tr>
<td>3123427</td>
<td>[CVE-2022-22532] HTTP Request Smuggling in SAP NetWeaver i</td>
<td>10</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>22.03.22</td>
<td>08.02.2022</td>
<td>JAVA</td>
</tr>
<tr>
<td>3080567</td>
<td>[CVE-2021-38162] HTTP Request Smuggling in SAP Web Dispatch</td>
<td>8.9</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>22.03.22</td>
<td>14.09.2021</td>
<td>Kernel/WebDispatcher</td>
</tr>
<tr>
<td>3149805</td>
<td>[CVE-2022-26201] Cross-Site Scripting (XSS) vulnerability in SAP</td>
<td>8.2</td>
<td>CVSS:3.0</td>
<td>Correction with high priority</td>
<td>22.03.22</td>
<td>08.03.2022</td>
<td>ABAP</td>
</tr>
</tbody>
</table>

#### March '22

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>CVSS Sc</th>
<th>CVSS Vi</th>
<th>Priority</th>
<th>Released</th>
<th>First Released</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3131047</td>
<td>[CVE-2021-44228] Central Security Note for Remote Code Execui</td>
<td>10</td>
<td>CVSS:3.0</td>
<td>Oi/HotNews</td>
<td>08.03.22</td>
<td>15.12.2021</td>
<td>Collective Note (Log4j)</td>
</tr>
<tr>
<td>3154684</td>
<td>[CVE-2022-44228] Remote Code Execution vulnerability associaci</td>
<td>10</td>
<td>CVSS:3.0</td>
<td>Oi/HotNews</td>
<td>08.03.22</td>
<td>08.03.22</td>
<td>Mobile</td>
</tr>
<tr>
<td>3149805</td>
<td>[CVE-2022-26101] Cross-Site Scripting (XSS) vulnerability in SAI</td>
<td>8.1</td>
<td>CVSS:3.0</td>
<td>Oi/Correction with high priority</td>
<td>08.03.22</td>
<td>08.03.22</td>
<td>ABAP</td>
</tr>
<tr>
<td>3145987</td>
<td>[CVE-2022-24396] Missing Authentication check in SAP Focuse</td>
<td>9.3</td>
<td>CVSS:3.0</td>
<td>Oi/HotNews</td>
<td>08.03.22</td>
<td>08.03.22</td>
<td>Hostagent / Simple Diagnostic Agent</td>
</tr>
<tr>
<td>3123396</td>
<td>[CVE-2022-22536] Request smuggling and request concatenati</td>
<td>10</td>
<td>CVSS:3.0</td>
<td>Oi/HotNews</td>
<td>08.03.22</td>
<td>08.02.2022</td>
<td>Kernel/WebDispatcher (only Textupdate)</td>
</tr>
</tbody>
</table>
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.
Validation of the Age of Support Package
based on SP Release-to-Customer date of any Software Component known in SAP PPMS***

**Technical Systems - Items: 5**

<table>
<thead>
<tr>
<th>Compliant</th>
<th>Customer</th>
<th>System ID</th>
<th>System Type</th>
<th>% Non Compliant</th>
<th># Non Compliant</th>
<th># Compliant</th>
<th>IT Admin Role</th>
<th>Lifecycle Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>DLM</td>
<td>MT8DLM</td>
<td>Application Server Java</td>
<td>0</td>
<td>0</td>
<td>66</td>
<td>Undefined</td>
<td>Active</td>
</tr>
<tr>
<td>Yes</td>
<td>DLM</td>
<td>N72DLM</td>
<td>Application Server Java</td>
<td>0</td>
<td>0</td>
<td>133</td>
<td>Demo System</td>
<td>Active</td>
</tr>
<tr>
<td>Yes</td>
<td>SSC</td>
<td>FQI5SC</td>
<td>Application Server Java</td>
<td>0</td>
<td>0</td>
<td>69</td>
<td>Production System</td>
<td>Active</td>
</tr>
<tr>
<td>Yes</td>
<td>Tyrelli Motors</td>
<td>JC5TMO</td>
<td>Application Server Java</td>
<td>0</td>
<td>0</td>
<td>66</td>
<td>Undefined</td>
<td>Active</td>
</tr>
<tr>
<td>Yes</td>
<td>Tyrelli Motors</td>
<td>JC6TMO</td>
<td>Application Server Java</td>
<td>0</td>
<td>0</td>
<td>66</td>
<td>Undefined</td>
<td>Active</td>
</tr>
</tbody>
</table>

***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
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)

Store Customizing
Policy Creation
Policy Scheduling
Alert Configuration
Maintain Exceptions
Alert Processing

© 2021 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
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.
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)
OCC Dashboard – Example

Operations Control Center (almdemo.com)
OCC Dashboard – Example

Operations Control Center (sap.corp)

Exceptions (Debug/Replace events)

CSA Policies (Baseline Compliance per Topic)

CSA Alerts (stacked by System)

CSA Policies (Baseline Compliance per System)
Security Dashboard

Debug & Replace Activities per system

<table>
<thead>
<tr>
<th>Date</th>
<th>FBT</th>
<th>FA7</th>
<th>E73</th>
<th>E2E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 4, 2022 4:00:00 PM</td>
<td>1,106</td>
<td>602</td>
<td>1,726</td>
<td>1,679</td>
</tr>
<tr>
<td>Apr 4, 2022 5:00:00 PM</td>
<td>1,124</td>
<td>756</td>
<td>1,899</td>
<td>1,899</td>
</tr>
<tr>
<td>Apr 4, 2022 6:00:00 PM</td>
<td>1,099</td>
<td>776</td>
<td>1,899</td>
<td>1,899</td>
</tr>
<tr>
<td>Apr 4, 2022 7:00:00 PM</td>
<td>1,102</td>
<td>732</td>
<td>1,914</td>
<td>1,914</td>
</tr>
<tr>
<td>Apr 4, 2022 8:00:00 PM</td>
<td>1,053</td>
<td>743</td>
<td>1,832</td>
<td>1,832</td>
</tr>
<tr>
<td>Apr 4, 2022 9:00:00 PM</td>
<td>1,045</td>
<td>768</td>
<td>1,841</td>
<td>1,841</td>
</tr>
<tr>
<td>Apr 4, 2022 10:00:00 PM</td>
<td>1,139</td>
<td>733</td>
<td>1,889</td>
<td>1,889</td>
</tr>
<tr>
<td>Apr 4, 2022 11:00:00 PM</td>
<td>1,154</td>
<td>774</td>
<td>1,944</td>
<td>1,944</td>
</tr>
<tr>
<td>Apr 5, 2022 12:00:00 AM</td>
<td>1,094</td>
<td>784</td>
<td>1,914</td>
<td>1,914</td>
</tr>
<tr>
<td>Apr 5, 2022 1:00:00 AM</td>
<td>1,129</td>
<td>746</td>
<td>1,895</td>
<td>1,895</td>
</tr>
</tbody>
</table>

Configuration & Security Analysis Alerts

<table>
<thead>
<tr>
<th>Date</th>
<th>FA7</th>
<th>E2E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 4, 2022 4:00:00 PM</td>
<td>53</td>
<td>55</td>
</tr>
<tr>
<td>Apr 4, 2022 5:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 4, 2022 6:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 4, 2022 7:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 4, 2022 8:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 4, 2022 9:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 4, 2022 10:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 4, 2022 11:00:00 PM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 5, 2022 12:00:00 AM</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Apr 5, 2022 1:00:00 AM</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Number of Security Alerts

234 Alerts

% of Non Compliant Items per Policy (ABAP)

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

Overall Compliancy %

46.91% Non Compliant
53.09% Compliant
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
Thank You!
Thank you.

Contact information:

Dr. Hendrik Mueller
SAP SE
hendrik.mueller@sap.com