Security

... or how best to protect your data and keep the availability of your SAP solutions

SAP CoE Security Services
January 2020
Abstract

Software security remains a critical topic of interest to all companies and to the information technology industry.

The security of a specific system thereby also significantly depends on the secure installation and operation of this system. SAP gained a lot of experience from its support for and engagement with numerous customers. It uses the resulting best practices not only for further improvements and enhancements of its support offering but also makes them available as recommendations, services and tools directly to its customers.

This presentation provides an introduction and overview of the content, tools and service from the SAP Center of Excellences - Security Services group.

More detailed slide decks are available for the topic areas of

- Security Patch Process
- Security Configuration and Authorization
Agenda

- Best Practices-based Services
- SAP Security Engagement

Security Tools and Services
- EarlyWatch Alert (EWA) – Security Chapter
- Security Optimization Service (SOS)
- Configuration Validation

- SAP Enterprise Support Report
- Secure Support Services
Typical Challenges remain the same!

- BUSINESS CONTINUITY
- BUSINESS PROCESS IMPROVEMENT
- PROTECTION OF INVESTMENT AND ACCELERATED INNOVATION
- REDUCED TOTAL COST OF OPERATION
- . . . and Security is an integral part!
Business case SAP Security

Why do you need to invest in SAP Security?
Business case SAP Security

What are the threats? Hackers, market competitors and even own employees. They might start:

- Ethical hacks.
- Industry espionage.
- Fraud schemes.
- Remember, 2/3 of data losses occur internally, either done intentionally or non-intentionally.
- Surveys found out that up to 4% of the employees might work against their own company.
- Recent cyber attacks were based on internal weaknesses: direct involvement of internal employees or at least taking advantage of internal accounts.

Recent, publicly know (non-SAP) attacks include:

- An internal employee of a national army copied confidential material
- An encryption specialist company was target of a cyber attack
- An external employee, working for a big organization, copied confidential material
- Big telco: an external admin reportedly stole 2.9 million user account data, incl. credit card details. They claimed that the credit card data were encrypted but were not 100% sure.
- Lots of other cases not made public.
Business case SAP Security

What is the benefit/added value of SAP security in general?
- Better reputation? => Possibly. Because, being hacked and losing data is no good press.

What are the challenges?
- In the first place, SAP Security requires investments. i.e., money, licenses, training.
- Second, SAP Security is a continuous process. Don’t stop!

IT Security and Data Protection must be guaranteed. Period.
- There is no excuse: You have to be compliant. And you have to proof that continuously.
- Being aware of security issues and doing nothing is no option anymore!

Compliance with national and international laws and agreements with business partners (e.g. export regulations, non-compliance can result in heavy legal (prison) terms and financial fines)

Costs after being hacked
- Direct costs: downtime of core business processes, handling/recovery of damaged/lost data.
- Indirect costs: reputation loss, brand/share value goes down
The Pillars of Product Security

- Security Functions
- Security Quality
- Secure Cloud Operations
- Secure Customer Operations
SAP Center of Excellences - Security Services
Our Mission

We support our customers
to efficiently design, build and run
their SAP systems and landscapes
in a secure manner
<table>
<thead>
<tr>
<th>Secure Operations Map</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization</strong></td>
</tr>
<tr>
<td>Awareness</td>
</tr>
<tr>
<td>Security Governance</td>
</tr>
<tr>
<td>Risk Management</td>
</tr>
<tr>
<td><strong>Processes</strong></td>
</tr>
<tr>
<td>Regulatory Process</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>Data Privacy &amp;</td>
</tr>
<tr>
<td>Protection</td>
</tr>
<tr>
<td>Audit &amp; Fraud</td>
</tr>
<tr>
<td>Management</td>
</tr>
<tr>
<td><strong>Application</strong></td>
</tr>
<tr>
<td>User &amp; Identity</td>
</tr>
<tr>
<td>Management</td>
</tr>
<tr>
<td>Authentication &amp;</td>
</tr>
<tr>
<td>Single Sign-On</td>
</tr>
<tr>
<td>Roles &amp; Authorizations</td>
</tr>
<tr>
<td>Custom Code Security</td>
</tr>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>Security Hardening</td>
</tr>
<tr>
<td>Secure SAP Code</td>
</tr>
<tr>
<td>Security Monitoring</td>
</tr>
<tr>
<td>&amp; Forensics</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
</tr>
<tr>
<td>Network Security</td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>&amp; Database Security</td>
</tr>
<tr>
<td>Client Security</td>
</tr>
</tbody>
</table>
Key Success Factors for Security

- Be aware of the invisibility of missing security

- Security requires support by everyone
  - It can't be delegated to a dedicated group

- Everyone
  - Must be aware that his/her support for security is essential
  - Must be motivated to support security
  - Must be enabled to support security

- Top Management support is key
  - Management support for groups and activities on security
  - Exemplary security behavior by management
Best Practices-based Services

- **Support**
  - Security Landing Page and Media Library
  - Security Guides
  - Security Whitepapers
  - Secure Operations Map

- **Customer Engagement**
  - Security Optimization Remote Service
  - Security Optimization Onsite Service
  - EGI Security Optimization Service (SOS)™
  - EGI Configuration Validation
  - EGI (Solution Manager) Roles and Authorization Concept

- **Service Delivery**
  - Security in EarlyWatch Alert
  - System Recommendations
  - Security Optimization Self Service
  - Security in Configuration Validation
  - Security Monitoring

- **Recommendations Guidelines**
  - Security Guides
  - Security Whitepapers
  - Secure Operations Map

- **Services delivered by SAP**
  - Security Optimization Remote Service
  - Security Optimization Onsite Service
  - EGI Security Optimization Service (SOS)™
  - EGI Configuration Validation
  - EGI (Solution Manager) Roles and Authorization Concept

- **Tools Self-Services**
  - Security in EarlyWatch Alert
  - System Recommendations
  - Security Optimization Self Service
  - Security in Configuration Validation
  - Security Monitoring
Security Management – continuous process along a Quality Circle

Analyze the differences and determine their root cause. Determine where to apply changes that will lead to improvements and the expected results.

Establish the objectives and processes necessary to deliver results in accordance with the expected output.

Measure the new processes and compare the results via indicators (KPIs) against the expected results in order to identify possible differences.

Implement the new processes and procedures.

The security plans (Plan) are implemented (Do) and the implementation is then evaluated (Check). After the evaluation both plans and implementation of the plan are carried out (Act).
For each IT organization:

1. Collect and document all systems maintained/operated.
   - Monitor changes in processes, infrastructure and risk situation.

2. All systems have to be assigned to a category of systems according the criticality of the data/information stored/processed on the system.

3. The IT security measures based on the system classification have to be aligned with the business requirements. Compromises might have to be made on both sides.
   - Remaining risks have to be identified and addressed with respective business owners.

4. Compare implemented security measures vs. security requirements and identify existing gaps.

5. Evaluate the operational risk resulting from the identified gaps.
   - Report the results of the risk assessment according the defined operational IT Risk Management process.

6. Develop an implementation plan covering the missing IT Security measures according the criticality of the related risk to be mitigated.
   - Implement the security measures.

- Collect and document all systems maintained/operated.
- Monitor changes in processes, infrastructure and risk situation.
### Analysis + Reporting

Company wide consolidation of security settings.

#### Authentication

Prove who you are. Passwords, SSO, Federation.

#### User Management

Maintain accounts. Identity Management and more.

#### Authorizations

Who’s allowed to do what? Privilege management.

#### System + Infrastructure Security

Code security, RFC gateway, network and interfaces.

---

- Develop an implementation plan covering the missing IT Security measures according to the criticality of the related risk to be mitigated.
- Implement the security measures.
- Evaluate the operational risk resulting from the identified gaps.
- Report on the risk assessment according to the defined operational IT Risk Management process.
- Collect and document all systems maintained/operated.
- Monitor changes in processes, infrastructure and risk situation.

---

**Investment on authorizations and user management (“putting locks on doors”)** often endangered by negligent handling of baseline security measures (“leaving open the windows”).

---

- The IT security measures based on the system classification have to be aligned with business requirements. Compromises might have to be made on both sides.
- Remaining risks have to be identified and addressed with respective business owners.

---

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Analysis+Reporting

Company wide consolidation of security settings.

- Develop an implementation plan covering the missing IT Security measures according the criticality of the related risk to be mitigated.
- Implement the security measures.
- Evaluate the operational risk resulting from the identified gaps.
- Report the results of the risk assessment according the defined operational IT Risk Management process.
- Collect and document all systems maintained/operated.
- Monitor changes in processes, infrastructure and risk situation.
- All systems have to be assigned to a category of systems according the criticality of the data/information stored/processed on the system.
- The IT security measures based on the system classification have to be aligned with the business requirements. Compromises might have to be made on both sides.
- Remaining risks have to be identified and addressed with respective business owners.

Internal and external auditors are “discovering” these topics at the moment!

System+Infrastructure Security

Code security, RFC gateway, network and interfaces.

For each IT organization

Inventory

Planning / Implementation

Information Classification

Risk Assessment

IT Security Requirements

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Agenda

➡ Best Practices-based Services

➡ SAP Security Engagement

Security Tools and Services

➡ EarlyWatch Alert (EWA) – Security Chapter
➡ Security Optimization Service (SOS)
➡ Configuration Validation

➡ SAP Enterprise Support Report

➡ Secure Support Services
How Collaboration Works
Establish a Cooperation with SAP

DElIVERY PROCEss FoLlOWS THE BASIC PRINCIPLES OF SAP MaxAttention ENGAGEMENTS

<table>
<thead>
<tr>
<th>360° Review</th>
<th>Benefit Case</th>
<th>Project Definition</th>
<th>Projects/ Services</th>
<th>Measurement &amp; Analytics</th>
<th>Reporting &amp; Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>holistic identification of areas for improvements and prioritization of focus areas.</td>
<td>baseline evaluation per focus area and anticipation of potential benefit</td>
<td>definition of project scope and milestones including required effort</td>
<td>execution of improvement project with customer and partners</td>
<td>Measure impact and result of the project activities</td>
<td>regular progress reporting as part of the SAP MaxAttention engagement reporting</td>
</tr>
<tr>
<td>agreement on key performance indicator</td>
<td>setup measurement of impact based on benefit case</td>
<td></td>
<td></td>
<td></td>
<td>Provide measurements of agreed KPIs as part of the quarterly reviews</td>
</tr>
</tbody>
</table>
SAP Security Engagement
General Approach

Top Topics named by customer, e.g. from audit reports

Security Checklist

New security-related information from SAP, e.g. from Security Whitepapers

Technical info of key production systems from EWA and SOS

Security Roadmap
SAP Security Engagement
General Approach – Security Roadmap

- Jan 10: Project Start
  - Workshop scheduled
  - Agenda agreed

- Feb 27: Security Workshop

- Mar 11, Mar 25: Workpackages start/end
- Apr 15, May 01, May 10: Roadmap signed off
- May 31: Implement finalized
- Jun 30: Project End

**Preparation**
- Scoping Call
- Roadmap Planning

**Roadmap Creation**
- Customer security situation and pain points
- Presentation of SOS findings
- Best practices for selected topics
- Identification & agreement on workpackages

**Implementation**
- Workpackage 1
- Workpackage 2
- Workpackage 3
- Workpackage 4
- Workpackage 5

**Verification**
- (bi-)weekly sync calls
- Security verification call or meeting
- Securing and documenting impact & achievements

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
SAP Security Engagement

Topics

➢ **Top Topics named by the customer** – typically those that triggered the interest in this service e.g. audit findings on security, a certain security incident, operational issues with security patching or authorization management or similar topics.

➢ **A Security Checklist** which allows for a security readiness evaluation against the most common recommendations and security measures. Together with Security Whitepapers from SAP and the SAP SES Secure Operations Standard comprising the Secure Operations Map this can be used for a 360 degree view on security in the workshop to not overlook significant security topics besides the already named topics.

➢ **New security information from SAP**: Not only systems change and develop but also the security and threat landscape around SAP systems evolve. Therefore SAP typically includes information on new security recommendations and options.

➢ **Technical info of key production systems**: To ground the often complex discussions around security it proved to be very helpful to have concrete technical security information from selected key production systems available in addition. This can e.g. be provided by corresponding EarlyWatch Alert Security chapters and a Security Optimization Service report prepared for the workshop.
Transparency and Mitigation
Empowering on available tools and content

Overview

Comparison against SAP recommendations
Security in EarlyWatch Alert (EWA)

Detail

Security Optimization Service System Recommendations

Company’s Security Policy

Company’s SAP Security Baseline

Target System

Configuration Validation

Management Dashboard

Comparison against company’s security policy

Service delivery example:

A Automated services indicate security gaps

Recommendation: Detailed look into gaps through experts

Service – Part 1:
- Root cause analysis for security gaps
- SAP Security Baseline maintenance

Service – Part 2:
- Security patch deployment cycle
- Configuration setup
- Proactive threat identification

Service – Part 3:
- Security control via dashboard
Expert Guided Implementation
“Training on the Job” at Its Best

Training, practical experience, remote consulting

Day 1

Training materials

Day 2

Empowering, Web session, 1-2 hours each morning

SAP expert explains step-by-step configuration using training materials

Execution, 2-3 hours on the same day

Participants execute demonstrated steps within their own project, on their own SAP Solution Manager software

Expertise on demand, during execution

Participants have direct access to an SAP expert who directly supports them remotely, if necessary, during the execution
Security-Related Expert Guided Implementation Sessions

- Guided Self Service “Security Optimization Service (SOS)”
- Configuration Validation
- Tools & Process Setup: Roles and Authorization Concept [for Solution Manager]
Agenda

➔ Best Practices-based Services
➔ SAP Security Engagement

Security Tools and Services
➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

➔ SAP Enterprise Support Report
➔ Secure Support Services
The Role of EarlyWatch Alert (EWA) for Security

SAP EarlyWatch Alert (EWA) (see https://service.sap.com/ewa)

SAP EarlyWatch Alert is an important part of making sure that your core business processes work. It is a tool that monitors the essential administrative areas of SAP components and keeps you up to date on their performance and stability. SAP EarlyWatch Alert runs automatically to keep you informed, so you can react to issues proactively, before they become critical.

Security in the EarlyWatch Alert:

- The EWA Report includes selected information on critical security observations
  - SAP Security Notes: ABAP and Kernel Software Corrections
  - Default Passwords of Standard Users
  - Password Policy
  - Gateway and Message Server Security
  - Users with Critical Authorizations
- More detailed and additional information can be found with the help of the security self-services
## EWA Summary

### ALERT OVERVIEW

- ![Alert](image) Secure password policy is not sufficiently enforced.
- ![Alert](image) Standard users including SAP* or DDIC have default password.
- ![Info](image) We found more than 30 ABAP dumps in your system.
- ![Info](image) Hardware resources may have been exhausted with the risk of performance degradation.
- ![Info](image) Security weaknesses identified in the Gateway or the Message Server configuration.
- ![Info](image) A high number of users have critical authorizations.

Based on these findings it is recommended that you perform the following Guided Self Services:

<table>
<thead>
<tr>
<th>Guided Self Service</th>
<th>FAQ</th>
<th>SAP Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Optimization Service</td>
<td></td>
<td>096478</td>
</tr>
</tbody>
</table>

### CHECK OVERVIEW

<table>
<thead>
<tr>
<th>Topic Rating</th>
<th>Topic</th>
<th>Subtopic Rating</th>
<th>Subtopic</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>Security</td>
<td>🔴</td>
<td>Default Passwords of Standard Users</td>
</tr>
<tr>
<td>🔴</td>
<td>Security</td>
<td>🔴</td>
<td>Control of the Automatic Login User SAP*</td>
</tr>
<tr>
<td>🔴</td>
<td>Security</td>
<td>🔴</td>
<td>ABAP Password Policy</td>
</tr>
<tr>
<td>🔴</td>
<td>Security</td>
<td>🔴</td>
<td>Gateway and Message Server Security</td>
</tr>
<tr>
<td>🔴</td>
<td>Security</td>
<td>🔴</td>
<td>Users with Critical Authorizations</td>
</tr>
</tbody>
</table>
10 Security

Critical security issues were found in your system. See the information in the following sections.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>☠️</td>
<td>SAP HANA System Privilege DATA ADMIN</td>
</tr>
<tr>
<td>☠️</td>
<td>SAP HANA Password Policy</td>
</tr>
<tr>
<td>☠️</td>
<td>SAP HANA Audit Trail</td>
</tr>
<tr>
<td>☠️</td>
<td>SAP HANA SQL Trace Level</td>
</tr>
<tr>
<td>✅</td>
<td>SAP Security Notes: ABAP and Kernel Software Corrections</td>
</tr>
<tr>
<td>✅</td>
<td>Default Passwords of Standard Users</td>
</tr>
<tr>
<td>✅</td>
<td>Control of the Automatic Login User SAP</td>
</tr>
<tr>
<td>☠️</td>
<td>ABAP Password Policy</td>
</tr>
<tr>
<td>🚫</td>
<td>Gateway and Message Server Security</td>
</tr>
<tr>
<td>☠️</td>
<td>Users with Critical Authorizations</td>
</tr>
</tbody>
</table>
EarlyWatch Alert Workspace in Support Portal Launchpad
https://launchpad.support.sap.com/#/ewaworkspace

SAP EarlyWatch Alert Workspace – gain an overview on your system landscape health

Note 2517661 - How to include EWA Fiori Cloud apps into customer launchpads
You can view the EWA Alerts in Support Portal Launchpad, i.e. you can search for “Security”

- **4 Systems**
  - **Gateway Security (Security ABAP Stack Gateway and Message Server Security)**
    - Gateway access control list (reg_info / sec_info) contains trivial entries (P TP=*, USER=*, USER-HOST=*, HOST=*).

- **6 Systems**
  - **Default Passwords of Standard Users (Security ABAP Stack)**
    - Standard users including SAP* or DDIC have default password.

- **14 Systems**
  - **SAP HANA Network Settings for Internal Services (Security SAP HANA Database HPJ)**
    - SAP HANA internal network configuration is insecure.

- **2 Systems**
  - **SAP HANA Network Settings for System Replication Communication (listeninterface) (Security SAP HANA Database P22)**
    - SAP HANA network settings for system replication is insecure.

- **22 Systems**
  - **ABAP Password Policy (Security ABAP Stack)**
    - Secure password policy is not sufficiently enforced (login/min_password_lng and login/password_max_idle_initial).

- **6 Systems**
  - **Gateway Security (Gateway and Message Server Security)**
    - Gateway Access Control List (reg_info / sec_info) contains trivial entries (P TP=*).

- **22 Systems**
  - **Users with Critical Authorizations (Security ABAP Stack)**
    - A high number of users has critical authorizations.

- **15 Systems**
  - **Default Passwords of Standard Users (Security ABAP Stack)**
    - Standard users other than SAP* or DDIC have default password.

- **3 Systems**
  - **Protection of Passwords in Database Connections (Security ABAP Stack)**
    - Protection of passwords in database connections (note 1823566).

- **3 Systems**
  - **SAP HANA SSFS Master Encryption Key (Security SAP HANA Database)**
    - SAP HANA SSFS master encryption key is not changed (note 2183624).
Agenda

➔ Best Practices-based Services

➔ SAP Security Engagement

Security Tools and Services

➔ EarlyWatch Alert (EWA) – Security Chapter

➔ Security Optimization Service (SOS)

➔ Configuration Validation

➔ SAP Enterprise Support Report

➔ Secure Support Services
SAP Security Optimization Service – Value Proposition

The SAP Security Optimization Service is designed to verify and improve the security of the SAP systems of customers by identifying potential security issues and giving recommendations on how to improve the security of the system.

Keeping the security and availability of customer SAP solutions high is a tremendous value to customers' businesses - a value delivered by the SAP Security Optimization Service. Analysis is the key to this value, which is necessary to:

- Decrease the risk of a system intrusion
- Ensure the confidentiality of business data
- Ensure the authenticity of users
- Substantially reduce the risk of costly downtime due to wrong user interaction

More information can be found under the alias SOS in the SAP Service Market Place

- [https://support.sap.com/sos](https://support.sap.com/sos)
The SAP Solution Manager offers the possibility to locally execute the SAP Security Optimization Service.

- All completely automated checks in ABAP systems
- No additional costs for this service

Broad range of security checks extending the Self-Service checks
- Performed by experienced service engineers
- Part of CQC service offering

Individual range of security checks, e.g. for the SAP Enterprise Portal
- Performed by specialists
- Additional costs for this service
Security Optimization Service
Scope of Remote Service and Self Service

SAP NetWeaver Application Server ABAP
- Basis administration check
- User management check
- Super users check
- Password check
- Spool and printer authorization check
- Background authorization check
- Batch input authorization check
- Transport control authorization check
- Role management authorization check
- Profile parameter check
- SAP GUI Single Sign-On (SSO) check
- Certificate Single Sign-On (SSO) check
- External authentication check

SAProuter
- SAProunttab checks
- OS access checks
- SNC checks

SAP NetWeaver Application Server Java
- Configuration checks
- SSL checks
- Administration checks

SAP Enterprise Portal
- Configuration checks
- Administration checks
- Authorization checks for portal content, user management and administration

Scope of the SOS Self Service

Types of checks in SOS NW AS ABAP
- Authorization checks: 116
- Non authorization checks: 110
  - Configuration checks: 66
  - Other security checks: 44
In order to determine the actual risk, the vulnerabilities are ranked using a rating logic. The rating is based on the severity and probability of each vulnerability. A report is created containing the identified vulnerabilities of the analyzed SAP system. The report contains recommendations to eliminate or reduce the vulnerabilities found during the Security Optimization Service.

The implementation of the recommended security measures can be done:
- By the customer
- By SAP security consulting
- By certified SAP partners
The questionnaire is filled out by the customer to prepare the service. The questionnaire contains about 25 questions. Specification of known users with critical authorizations in the questionnaire skips them from the report. This helps to keep the report readable and to do a correct risk analysis. Customize the look of the report. Selection of the tested clients.
Guided Self-Service for Security Optimization

Execute Session

Security Optimization Service

Session Number: 200000032204  User Name: BUCHHOLZF

Steps

<table>
<thead>
<tr>
<th>Status</th>
<th>Updates Needed</th>
<th>Description</th>
<th>Last Changed at</th>
<th>Last Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td></td>
<td>Select System</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select Login to Managed System</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assign Questionnaire</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Choose/Schedule Data Collection</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
</tbody>
</table>

Help

In this step you will prepare your session.

It is divided in several substeps, in which you’ll find detailed description.

Choose always ‘Next’ to continue and to go through the session.

Below ‘Steps’ you’ll find an overview of the substeps with additional information like status, changed date and time,...
Customer Report: Service Rating

The Security Optimization Self Service results in a report which contains all identified findings, enhanced with corresponding recommendations.

If very critical issues are found, then the overall SOS rating will be red. In this case, the chapter “Service Rating” will list those checks that triggered the overall red rating.

3 Service Rating

Severe critical security issues were found in your system. See the information in the following sections.

The following list provides an overview of the selected checks that are decisive for the severe critical ("RED") rating of this service.

CHECKS DECISIVE FOR SEVERE CRITICAL ("RED") RATING

<table>
<thead>
<tr>
<th>Check Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>User SAP* has the default password in some clients (0041)</td>
</tr>
<tr>
<td>User DDIC has the default password in some clients (0048)</td>
</tr>
<tr>
<td>Security Audit Log is not active (0170)</td>
</tr>
<tr>
<td>Minimum Password Length (0126)</td>
</tr>
<tr>
<td>Additional Super User Accounts Found (0022)</td>
</tr>
<tr>
<td>Users Authorized to Debug / Replace (0308)</td>
</tr>
<tr>
<td>Users Authorized to Maintain All Tables (0514)</td>
</tr>
<tr>
<td>Users Authorized to Execute All Function Modules (0520)</td>
</tr>
<tr>
<td>System Change Option (0301)</td>
</tr>
</tbody>
</table>
The action items list on top of the report gives a good overview about the complete system status. The action items are created automatically of all checks rated with high risk. The list can be individually adapted. We use the red traffic light as “high risk” and the yellow traffic light as “medium risk.” “Green” results are normally skipped in order to reduce the size of the report.

All checks have a four-digit identifier which allows to find the detailed description in the report easily.
Deriving an Action Plan

Deriving an Action Plan is easy ... in theory.

The SOS report is designed to already contain everything you need for it:
- a general introduction
- the findings and explanations
- risk ratings
- recommendations
- technical background information

So just go ahead!

For each check in the SOS report:
1. analyze the reason and validity of the finding
2. maintain the questionnaire where appropriate
3. take corrective action based on the recommendation
Deriving an Action Plan
... is not that easy when the report is huge

When the SOS report is huge
- working on it as described on the slide before takes a lot of time and resources
- ... and may even cause that nothing happens at all.

The goal of the SOS however is not to produce a nice report but to have impact and improve the security of the respective system!

Recommended solution:
- Identify „Top Issues“ – including those potentially listed in the “Service Rating” chapter – and solve them first!
- Identify „Systematic Issues“ (e.g. issues with the authorization concept) and trigger a solution
- Identify „Quick Wins“ and implement them
- Determine the remaining risk and
  - either address the next set of „Top Issues“
  - or get agreement, that the achieved level of security looks acceptable until the next scheduled run of the SOS
Agenda

➔ Best Practices-based Services
➔ SAP Security Engagement

Security Tools and Services
➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

➔ SAP Enterprise Support Report
➔ Secure Support Services
Consider Customers Situation of Today …

Are the OS, DB, Software and Kernel on the certain / latest level? … on all Systems? .. Please show me?

Are all our CRM systems compliant with the new Configuration Baseline?.. not compliant.. which systems? what exactly?

Have we applied SAP Note xxxxx on all systems? …please report implementation status for all systems?

Have we imported Transport request xxxx (with important performance changes) on all systems? … could I have a list of the systems where it is still missing?

Are security settings applied? …on all systems? … could you please confirm and report?

Challenges

• A large number of systems… Complex SAP Landscape …
• … Need to perform comparison of current configuration status against a defined target or standard configuration baselines
• … with minimum efforts and ASAP
The Diagnostics Core
Diagnostic Infrastructure

Solution Manager

- BI Reporting
- InfoCube: OSMD_CA02
- E2E Change Analysis II

Extractor Framework (EFWK)
- Hourly

Configuration and Change Database (CCDB)

Managed System

- Non-ABAP based installations
  - Diagnostics Agents
- ABAP based installations
  - Extractor Framework once a day
  - Solution Tool Plugins (ST-A/PI)

The extraction of the data is scheduled as soon as a “Managed System Configuration” has been performed for a system.

1. **E2E Change Analysis – Top-Down View on Changes**
   - Drilldown navigation

2. **Change Reporting – Browse CCDB data**
   - CCDB data view
What is Configuration Validation?

The Idea behind Configuration Validation

A reporting to understand how homogeneous the configuration of systems is

Reference System

- Configuration Items
  - Software Packages
  - ABAP Notes
  - Kernel level
  - Transports
  - Parameters

Configuration Validation

Compared Systems

System 1
- Configuration Items
  - ABAP Notes
  - Software Packages
  - Transports
  - Parameters

... System N
- Configuration Items
  - ABAP Notes
  - Software Packages
  - Transports
  - Parameters

Typical questions are:

- All systems on a certain OS level or DB level?
- Template configuration (SAP or DB parameter) applied on all systems?
- No kernel older than 6 month on all systems?
- Security policy settings applied? Security defaults in place?
- Have certain transports arrived in the systems?
<table>
<thead>
<tr>
<th>Content Deliverables – Configuration Items Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software Release Validation</strong></td>
</tr>
<tr>
<td>Application</td>
</tr>
<tr>
<td>• Support Package Stack</td>
</tr>
<tr>
<td>• Software Component Versions</td>
</tr>
<tr>
<td>• Implemented SAP Notes</td>
</tr>
<tr>
<td>• Imported ABAP Transports</td>
</tr>
<tr>
<td>Kernel</td>
</tr>
<tr>
<td>• Web AS ABAP Kernel Release</td>
</tr>
<tr>
<td>• Java VM version</td>
</tr>
<tr>
<td>• Web AS Java Release</td>
</tr>
<tr>
<td>Database</td>
</tr>
<tr>
<td>• Database Release</td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>• Operation System Release</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>• Operation System Environment Settings</td>
</tr>
<tr>
<td>Parameter Validation</td>
</tr>
<tr>
<td>SAP Product specific settings</td>
</tr>
<tr>
<td>• PI/XI specific configuration</td>
</tr>
<tr>
<td>• BI specific configuration</td>
</tr>
<tr>
<td>• BIA specific configuration</td>
</tr>
<tr>
<td>ABAP Instance Parameters</td>
</tr>
<tr>
<td>• Java VM parameters for J2EE</td>
</tr>
</tbody>
</table>

Security Parameters:
- Standard Users
- Gateway Secinfo
- Gateway Reginfo

Critical Auth. Profiles:
- Critical auth. profiles
- Critical authorizations
Big Picture: Reporting / Alerting / Management Dashboard

Configuration Validation Target Systems could be used in several areas

- Configuration Validation
- Management Dashboard
- Reporting
- System Monitoring / Alerting

Selected ConfigStores and Items - Only Non-compliant Items with Value and Target Value

<table>
<thead>
<tr>
<th>System</th>
<th>SID</th>
<th>Config Item</th>
<th>Config Item Value</th>
<th>Value of Target System</th>
<th>Compliance</th>
<th>Last Check (UTC)</th>
<th>Compliant (true=false)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FNE 000344</td>
<td>1028</td>
<td>authHeaderCallFunction</td>
<td>2</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>loginCalls_end_userLogin</td>
<td>0</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>loginCalls_end_commonUserlogin</td>
<td>0</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logEntry_password_crack</td>
<td>1</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logEntry_password_ssh</td>
<td>1</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logEntry_password_sftp</td>
<td>1</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logEntry_password_scp</td>
<td>1</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logEntry_password_key</td>
<td>1</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logEntry_password_scp</td>
<td>1</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>loginPassword_expiration</td>
<td>3</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>loginPassword_expiration</td>
<td>3</td>
<td>No</td>
<td>2013030110:00:15</td>
<td>FNE 000344</td>
<td>2013030110:00:15</td>
</tr>
</tbody>
</table>

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Agenda

➔ Best Practices-based Services
➔ SAP Security Engagement

Security Tools and Services
➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

➔ SAP Enterprise Support Report
➔ Secure Support Services
This section provides an overview over important security topics affecting your SAP systems.

**SECURITY (SAP SYSTEM ANALYSIS)**

1. Overview about Security in the Early Watch Alert Reports

2. Overview about the Security Optimization Service sessions
SAP Enterprise Support Report
Overview about Security in the Early Watch Alert Reports

This section provides an overview of diverse security alerts reported by SAP EarlyWatch Alert for your most important production systems. Implementation status of security-related SAP Notes and Hot News are being checked as well as the amount of users with critical authorizations and standard users with default passwords.

<table>
<thead>
<tr>
<th>System ID</th>
<th>Installation Number</th>
<th>Date of EWA</th>
<th>Security-related SAP Notes</th>
<th>Users with Critical Authorizations</th>
<th>Default Passwords of Standard Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>123456789</td>
<td>01.03.2010</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>DEF</td>
<td>234567890</td>
<td>01.03.2010</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>GHI</td>
<td>123456789</td>
<td></td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
</tbody>
</table>
The SAP Security Optimization Service is designed to verify and improve the security of the SAP systems by identifying potential security issues and giving recommendations on how to improve the security of the system.

The SAP Security Optimization Service can be used during the whole lifecycle of a system.

<table>
<thead>
<tr>
<th>System</th>
<th>Date of the SOS Session</th>
<th>Result</th>
<th>Description</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>✗</td>
<td>No Security Optimization Service was executed during the last year.</td>
<td>Consider to schedule a SAP CQC Security Optimization Service as a remote service (covers both ABAP &amp; Java).</td>
</tr>
</tbody>
</table>
Agenda

➔ Best Practices-based Services

➔ SAP Security Engagement

Security Tools and Services

➔ EarlyWatch Alert (EWA) – Security Chapter

➔ Security Optimization Service (SOS)

➔ Configuration Validation

➔ SAP Enterprise Support Report

➔ Secure Support Services
Secure Support Services
for SAP® Enterprise Support and SAP MaxAttention™

Scope
In response to the constantly growing demand for individual secure services of
• National defense and security organizations
• Public-sector authorities
• Aerospace and defense companies
• Banking and insurance companies
• High-tech companies
and beyond, we created the complementary secure support services offering for SAP Enterprise Support and SAP MaxAttention customers.

Advanced Security Requirements
Our support organization has special expertise and over 10 years experience in delivering secure support for high-security environments. With secure support services you can now benefit from the full range of SAP support services regarding message solving, remote support and data handling.

Service Packaging
As a packaged service offering, SAP secure support services allow bundling of features (e.g. customer-owned hardware, secure remote services, security-cleared personnel, secure rooms, etc.) to satisfy your individual security requirements and data policies!

Message Solving
From the processing of unclassified messages with restricted remote access for system analysis up to the handling of classified messages.

Remote Support
Remote system access and remote analysis from defined countries or locations meeting our customer’s own special data security policy or legal regulations.

Data Handling
Integration of security-cleared support personnel, special secured rooms in SAP locations and the ability to classify support messages for further processing.

service.sap.com/securesupport
Thank You!

Contact information:
SAP CoE Security Services
securitycheck@sap.com