

# SAP CYBERSECURITY BEST PRACTICES & IMPLEMENTATION CHALLENGES

**Nipun Mahajan**, Senior Cybersecurity Analyst, Lonza

**Bill Oliver**, Managing Director, SecurityBridge



Las Vegas

---

2024

**SAP**insider



## In This Session

---

### SAP Cybersecurity the Key pillars

- SAP Security Position (Start Strong)
- SAP Security Patch Management
- Custom Code vulnerabilities
- Security Monitoring (Intrusion Detection)

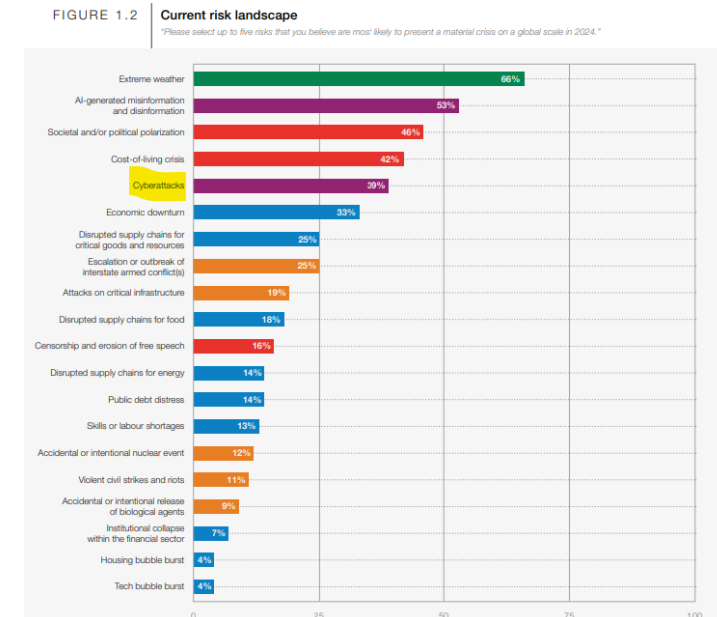
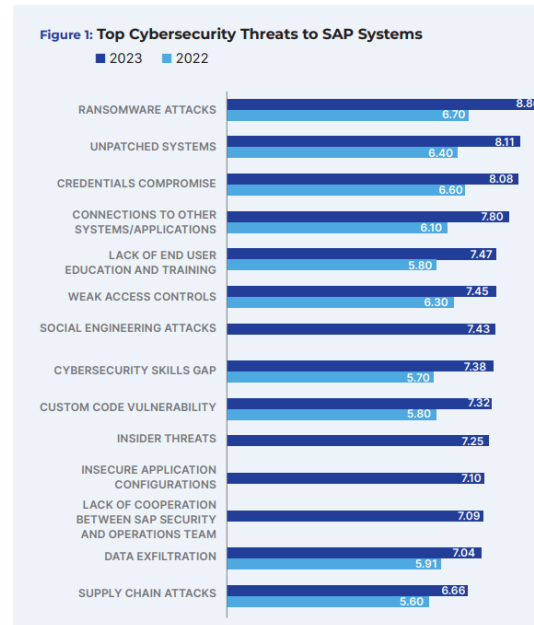
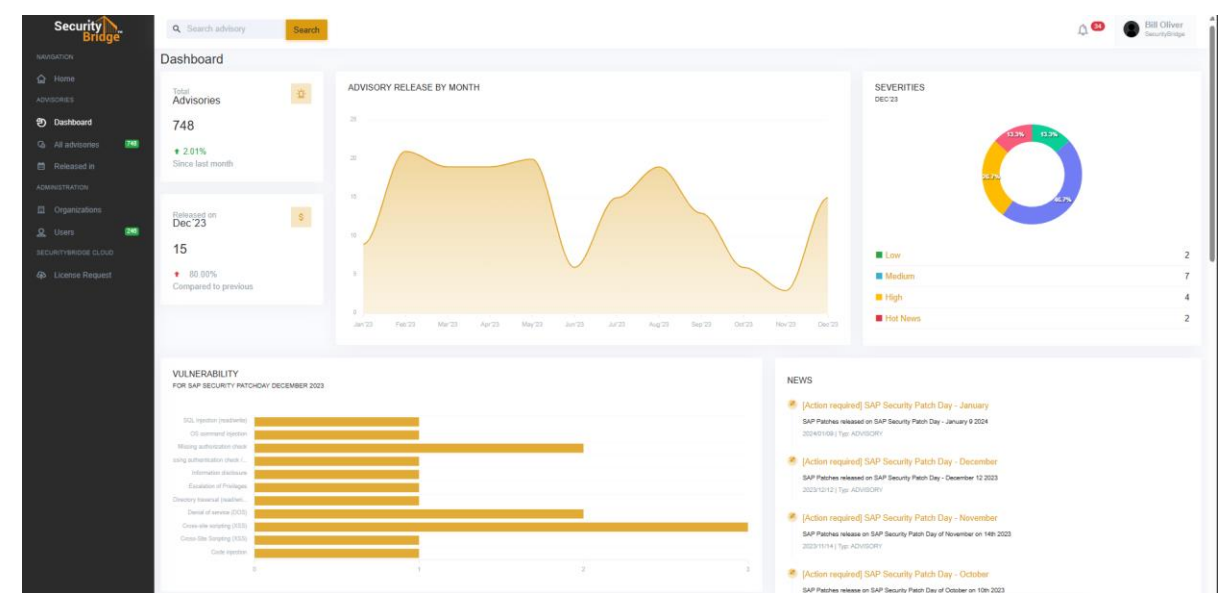
### Lonza's SAP Cybersecurity Journey



# SAP Security Surroundings

Has SAP ever been breached?

- **Between mid 2020 and March 2021, 300 out of every 1500 cyber-attacks were successful in exploiting target SAP systems**
- USIS breach, personnel records of federal employees and contractors with access to classified data
- Critical SAP Vulnerability Allows Supply Chain Attacks
- Critical SAP Vulnerabilities, CISA (Cybersecurity & Infrastructure Security Agency) suggests swift patching
- In 2023, SAP has released over 160 security patches 21 of which are classified as “Hot News.” SAP recommends implementation immediately.



Source: WEF Global Risk Report 2023

Source: <https://www.cpomagazine.com/cyber-security/hackers-exploit-known-sap-security-vulnerabilities-with-a-typical-cyber-attack-succeeding-in-record-time/>

Source: <https://sapinsider.org/research-reports/cybersecurity-threats-to-sap-systems>

---

# Hardening your SAP Security Position

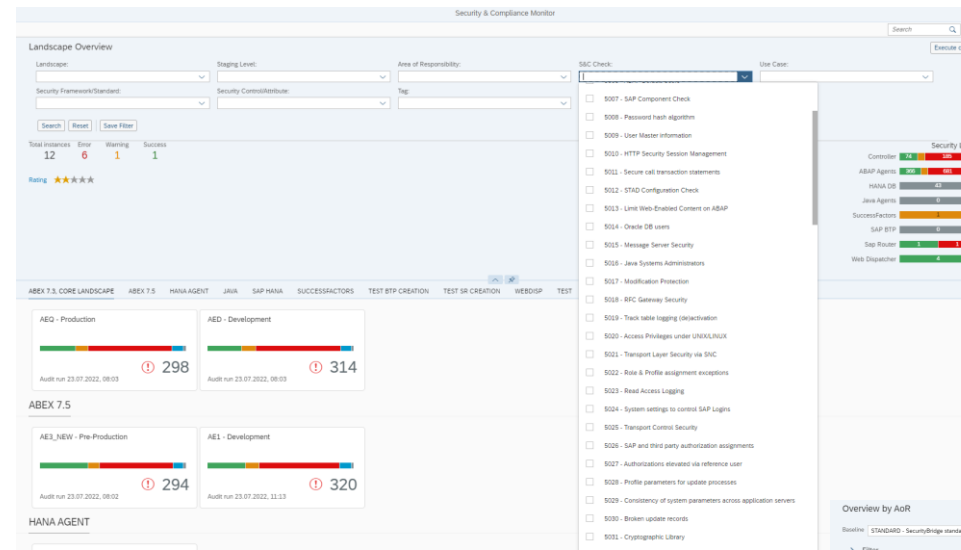


# Hardening your SAP Security Position

If you have not already started hardening your SAP Security position, you need to start now. This is more than just who has access to “SAP\_ALL”, who can run Profile Generator (PFCG), and what users can create and pay vendors (Segregation of Duties violations).

SAP System is so much more. A few of the many things you should look at are:

- Communication and Channel Security (RFC connections, HTTP connections, etc.)
- Internet Communications Framework
- File Systems Access Security
- Virus Scanning
- Data Storage Security (Encryption)
- Masking Data (Online presentation, Anonymization reporting)



PUBLIC  
SAP HANA Platform 2.0 SPS 05  
Document Version: 1.0 - 2021-05-21

## SAP HANA Security Guide for SAP HANA Platform

THE BEST RUN SAP

**Focused Run**  
The Ultimate Solution for Monitoring, Alerting, Root Cause Analysis, and Analytics

CUSTOMER/PARTNER



SAP Run Simple



---

# Security Patch Management




# SAP Security Patch Management

For those who don't know, SAP has what we call "Patch Tuesday." On the second Tuesday of every month, SAP releases Security patches. They break them up into four categories: Hot News, High, Medium, and Low.

In 2023, SAP has released over 160 security patches 21 of which are classified as “Hot News.” SAP recommends implementation immediately.

While it is up for debate on how quickly you need to install these patches. The key is not to leave this to your “Yearly Service Pack install and testing rollout.” I have seen suggestions for the timing to implement Security notes anywhere from 15 days (Hot News – Highest Security impact) to 180 days (Low Security impact). The key is faster the better.

| Note Category  | Priority  | Implementation Timing | Deadline | Deadline Notes / Comments  |
|----------------|-----------|-----------------------|----------|--|
| Hot News       | Very High | 15 days               | 30 days  | Based on Risk Potential  |
| Security Notes | High      | 30 days               | 60 days  |  |
|                | Medium    | 90 days               | 180 days |  |
|                | Low       | 180 days              | N/A      | Aligned to maintenance/support release planning and implementation |


[Support](#)

[My Support](#)
[Products](#)
[Tools](#)
[Maintenance](#)
[Offerings & Programs](#)
[ALM](#)
[Explore SAP](#)


[SAP Support Portal Home](#)
[My Support](#)
[Knowledge Base](#)

## SAP Security Notes & News

[Overview](#)
[Security Patch Day](#)
[Resources](#)

# SAP Security Notes

Review and implement critical SAP Security Notes, plan for upcoming SAP Security Patch Days




### SAP Security Notes

SAP Security Notes contain SAP's expert advice regarding important action items and patches to ensure the security of your systems.

[Access SAP Security Notes in the Launchpad](#)


[Access SAP Security Notes in SAP for Me](#)



### SAP Security Notes FAQs

Get your frequently asked questions regarding SAP security patching answered by reviewing our SAP Security Notes FAQs.

[Read FAQs](#)



### Report a Possible Security Vulnerability to SAP

SAP takes all matters relating to your security very seriously, and we are constantly working on improving our product security measures. If you discover a potential security vulnerability in any SAP Software then follow the guidelines here.

[Report a Vulnerability](#)

## SAP Security Patch Day

The security maintenance of installed SAP software is key to continuously protect also against new types of attacks or newly identified potential weaknesses.

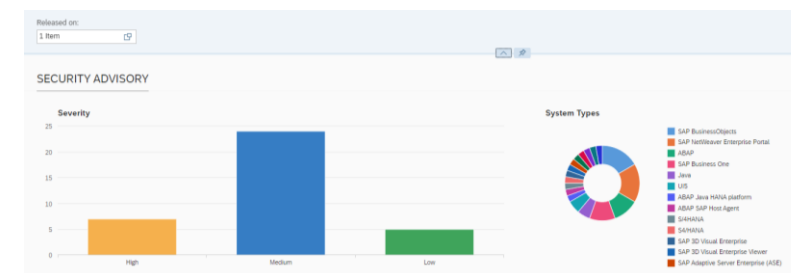
Based on feedback from customers, partners and SAP user groups, SAP has launched a regular SAP Security Patch Day, scheduled for the second Tuesday of every month – which has been synchronized with the Security Patch Day of other major software vendors.

On these SAP Patch Days, SAP publishes software corrections as SAP Security Notes, focused solely on security to protect against potential weaknesses or attacks. Access SAP Security Notes in the Launchpad, then select all SAP Security Notes, to get the complete list of all SAP Security Notes. We recommend that you implement these corrections at a priority. Several tools are available to help identify, select and implement these corrections.

SAP categorizes SAP Security Notes as *Patch Day Security Notes* and *Support Package Security Notes*, with the same amount of availability and importance invested from our side with these two types of updates.


### Planned Dates for 2023 SAP Security Patch Days

|             |
|-------------|
| January 10  |
| February 14 |
| March 14    |
| April 11    |
| May 9       |
| June 13     |
| July 11     |
| August 8    |



# Security Advisories

## Cloud.SecurityBridge.com



NAVIGATION

Home

ADVISORIES


Dashboard

All advisories 590

Released in

Search advisory

Search



### Security Advisories

We've created the first of its kind, SecurityBridge Cloud Platform to prioritize SAP patches, updates and the remediation strategies essential for preventing the disruption of vital business systems. Our security advisories enable SAP users to understand the security and business implications of running SAP.

The user interface, is designed to be as intuitive as possible but we'd love to hear your feedback and [opinions](#). We hope you like it!

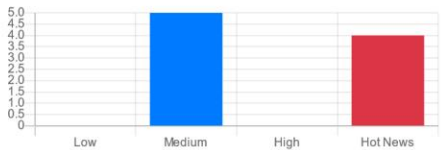
Patchdays 2023 ▾ 2022 ▾ 2021 ▾ 2020 ▾ 2019 ▾ 2015 ▾

Yikes, there is work to do!

This time we found critical correction advisories. We count 9 and the highest CVSS score is 9.9.


Severity

SAP® Security advisories 9



System Types

Affected SAP® system types




Related note

3275391

CVSS

9.9



Affected system type

SAP Business Planning...

Patchday

2023-01

Released on


2023/01/10

Related note

3262810

CVSS

9.9



Affected system type

BI/BO platform

Patchday

2023-01

Released on


2023/01/10

Related note

3268093

CVSS

9.4



Affected system type

Java

Patchday

2023-01

Released on

2023/01/10

8

SAPinsider



---

# Custom code Vulnerabilities



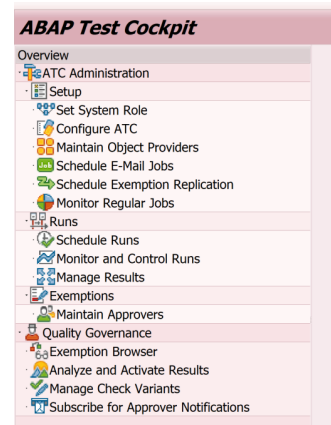
# Custom Code Vulnerabilities

Now that we know how SAP fixes code (Patch Management), the question becomes, *“How are you going to fix all that custom ABAP you have been doing over the years that have security issues?”*

“Are you actually reviewing your custom code for Security defects?” If not (a common response is “What is a Code Scan?”), then you need to start now.

A few things to look for:

- *SQL Injections*
- *Missing Authority checks*
- *Backdoor Injections*
- *Mass data deletion*
- *Key SAP Programs/function modules that should not be in Custom Code*
- *Test programs still in production*
- *Directory Traversal*



# Custom Code Vulnerabilities

Scanning custom code to ensure security risks are identified and addressed fully integrated within the SAP standard development process.



**ABAP Test Cockpit**

Overview

- ATC Administration
  - Setup
    - Set System Role
    - Configure ATC
    - Maintain Object Providers
    - Schedule E-Mail Jobs
    - Schedule Exemption Replication
    - Monitor Regular Jobs
  - Runs
    - Schedule Runs
    - Monitor and Control Runs
    - Manage Results
  - Exemptions
    - Maintain Approvers
  - Quality Governance
    - Exemption Browser
  - Analyze and Activate Results
  - Manage Check Variants
  - Subscribe for Approver Notifications

- Vulnerability type:
- ☐ SQL-Injection
- ☐ OS-Command execution
- ☐ Authority check validation
- ☐ Authority Check - CDS views
- ☐ Backdoor identification
- ☐ Backdoor identification on system client
- ☐ Backdoor identification on user
- ☐ Source Code Injection
- ☐ Standard table manipulation
- ☐ Directory Traversal
- ☐ Insecure Communication
- ☐ Critical Keywords
- ☐ Critical Keywords (Function)
- ☐ Critical Keywords (Program)
- ☐ Critical Keywords (SAP Directory)
- ☐ Critical Keywords (Transaction)
- ☐ Potential test object on dev-system
- ☐ Potential temporary/test program on non-dev-system
- ☐ Client Specific SHMM Objects

| Code Inspector: Results for ZGETHASH (PROG)                        |       |          |             |
|--|-------|----------|-------------|
|  | Error | Warnings | Information |
| List of Checks   | 15    | 1        | 0           |
| Performance Checks   | 0     | 0        | 0           |
| Security Checks  | 0     | 0        | 0           |
| Critical Statements  | 0     | 0        | 0           |
| Syntax Check/Generation  | 0     | 0        | 0           |
| Reduced Programming  | 0     | 0        | 0           |
| User Interfaces  | 0     | 0        | 0           |
| SecurityBridge Code Vulnerability Analyzer                         | 15    | 0        | 0           |
| SQL Injection (SecurityBridge)                                     | 1     | 0        | 0           |
| OS Command Injection (SecurityBridge)                              | 1     | 0        | 0           |
| Authority Check Vulnerabilities (SecurityBridge)                   | 1     | 0        | 0           |
| Backdoor Vulnerabilities (SecurityBridge)                          | 2     | 0        | 0           |
| Source Code Injection (SecurityBridge)                             | 1     | 0        | 0           |
| Standard Table Changes (SecurityBridge)                            | 1     | 0        | 0           |
| Directory Traversal Vulnerabilities (SecurityBridge)               | 1     | 0        | 0           |
| Insecure communication protocols (SecurityBridge)                  | 1     | 0        | 0           |
| Critical Keywords (SecurityBridge)                                 | 1     | 0        | 0           |
| Existence of potential TEST or TEMPORARY programs (SecurityBridge) | 1     | 0        | 0           |
| Client-Specific Shared Object Methods (SecurityBridge)             | 1     | 0        | 0           |
| Other Checks (SecurityBridge)                                      | 1     | 0        | 0           |





---

# Security Monitoring

# Security Monitoring

Monitoring what is happening right now in your SAP systems is something that every organization needs to be doing.

You need to look at this from an “I’ve been hacked” perspective.

While it’s important to monitor who ran what transactions in SAP and who created what POs, etc. your security team needs to know more about what’s happening in your SAP systems, which includes (but not limited to):

- Failed Logins from unknown accounts
- Debugging activated (in production systems)
- Security Audit Log changes (turn off, change scope of logging, etc.)
- Download critical tables
- Mass changes to critical tables
- Digital signature error
- RFC Callback rejected
- Suspicious HTTP calls

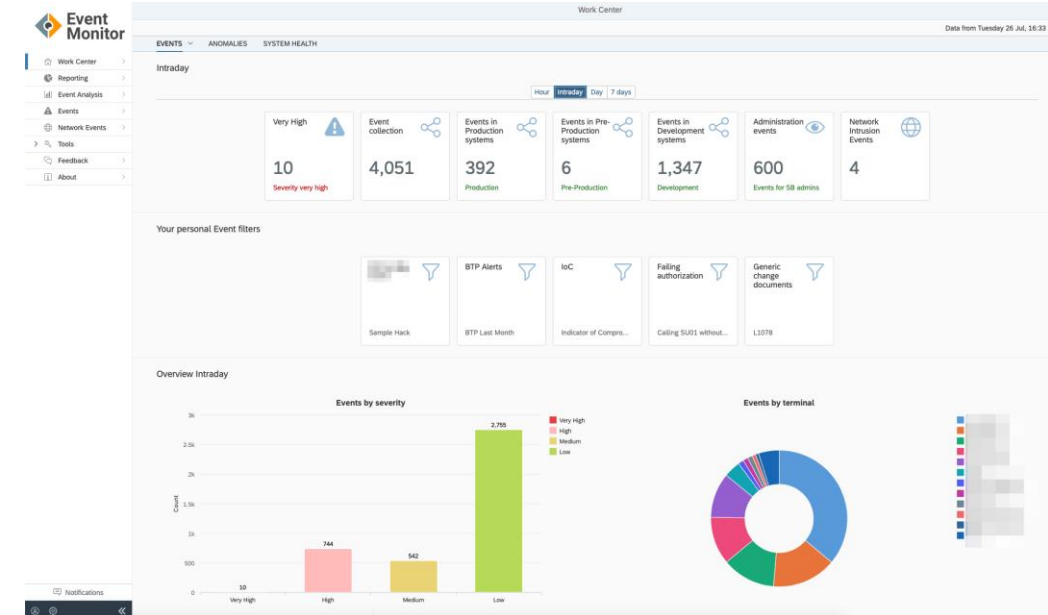
Analysis of Security Audit Log

Period Requested: 04.01.2019 20:00:00 - 04.01.2019 21:35:10  
Period Selected: 04.01.2019 21:28:05 - 04.01.2019 21:34:52  
Server: SAPMSM19

Audit Classes:


- Dialog Logon
- RFC/CPIX Logon
- RFC Function Call
- Transaction Start
- Report Start
- User Master Change
- Other Events
- System Events

| Creation Date | Date/Time | CL  | User    | Terminal name   | TCode | Program  | Audit Log Msg. Text                                      | Long Text | Proc. | WP  | Data | Data | Data |
|---------------|-----------|-----|---------|-----------------|-------|----------|--|-----------|-------|-----|------|------|------|
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Active status set to 1                            |           | D     | 006 | 1    |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: configuration changed                             |           | D     | 006 |      |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Slot 1 Inactive                                   |           | D     | 006 | 1    |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Slot 2 Inactive                                   |           | D     | 006 | 2    |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: configuration changed                             |           | D     | 006 |      |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Slot 1 Inactive                                   |           | D     | 006 | 1    |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: configuration changed                             |           | D     | 006 |      |      |      |
| 04.01.2019    | 21:28:05  | 600 | BOLIVER | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Slot 2 Inactive                                   |           | D     | 006 | 2    |      |      |
| 04.01.2019    | 21:34:52  | 600 | HACKER  | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: configuration changed                             |           | D     | 000 |      |      |      |
| 04.01.2019    | 21:34:52  | 600 | HACKER  | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Slot 1: Class 64, Severity 2, User " , Client " , |           | D     | 000 | 1    | 64   | 2    |
| 04.01.2019    | 21:34:52  | 600 | HACKER  | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: configuration changed                             |           | D     | 000 |      |      |      |
| 04.01.2019    | 21:34:52  | 600 | HACKER  | DESKTOP-1309NDD | SM19  | SAPMSM19 | Audit: Slot 2 Inactive                                   |           | D     | 000 | 2    |      |      |



# Now what ?

There will be times you don't want to just see it happen; you want to take action !



Work Center >

Reporting >

Event Analysis >

Events >

Network Events >

Tools >

Feedback >

About >

Events

Hour Intraday Day Week T 3d


Data from Friday, Feb 10, 19:44 (system time)

Filter

OFF

Refresh

Aggregate

| System  | Time                | Severity   | Listener  | Program & Transaction | User  | Terminal | Message | Options |     |
|---------|---------------------|------------|---|-----------------------|---|----------|---------|---------|-----|
| AE1 001 | 09.02.2023 19:30:38 | Medium (4) | 1094 Activity from one user involving multiple workstations | SAPMHTTP S000         |  |          |         |         | ... |
| AE1 001 | 09.02.2023 19:30:38 | Medium (4) | 1094 Activity from one user involving multiple workstations | SAPMHTTP S000         |   |          |         |         | ... |
| AE1 001 | 09.02.2023 18:38:21 | Medium (4) | 1094 Activity from one user involving multiple workstations | SAPMSYST S000         |   |          |         |         | ... |

Active: ☒

\*Action name: Drop User

Description:

\*Action Type:

\*Action timing: 

Send an email

\*Valid from: 

Show a popup to the user triggering the event

\*Valid to: 

Immediate lock account of the user initiating event

Incident Management

Mark as security irrelevant

Activate a trace for the user triggering the event

Kill all user session, system wide

Automatic development key deletion


Automatic deprovisioning of the role/profile

Set target severity

Hyperlogging



# Where is all my data going ?

- **Interface  
Traffic  
Monitor**
- Work Center >
  - Traffic >
  - RFC Recorder >
  - RFC Destinations >
  - Non Responding >
  - Production Paths >
  - Trusted Systems >
  - Data Extractions >
  - OData Services >
  - Feedback >

Work Center

Data from Friday, Feb 10, 20:02 (system time)

RFC Recorder

No. of systems

4 active

3 not active

Critical access paths (used)

4

Intraday7 days30 days

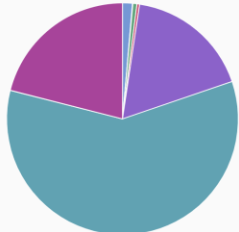
RFC destinations in use

26

Security relevant RFC calls

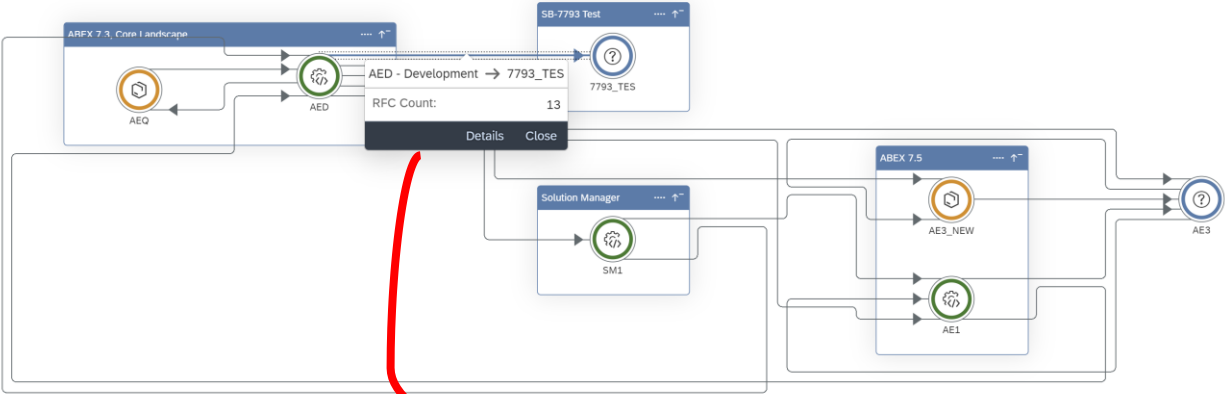
6,109

Last used RFC function calls



Total number of RFC calls by the system

| System  | Inbound calls | Outbound calls |
|---------|---------------|----------------|
| AE1     | 4,626         | 0              |
| AE3_NEW | 1             | 1              |
| AED     | 1,325         | 142            |
| AEQ     | 14            | 0              |



AED - Development → 7793\_TES

RFC traffic statistics (5)

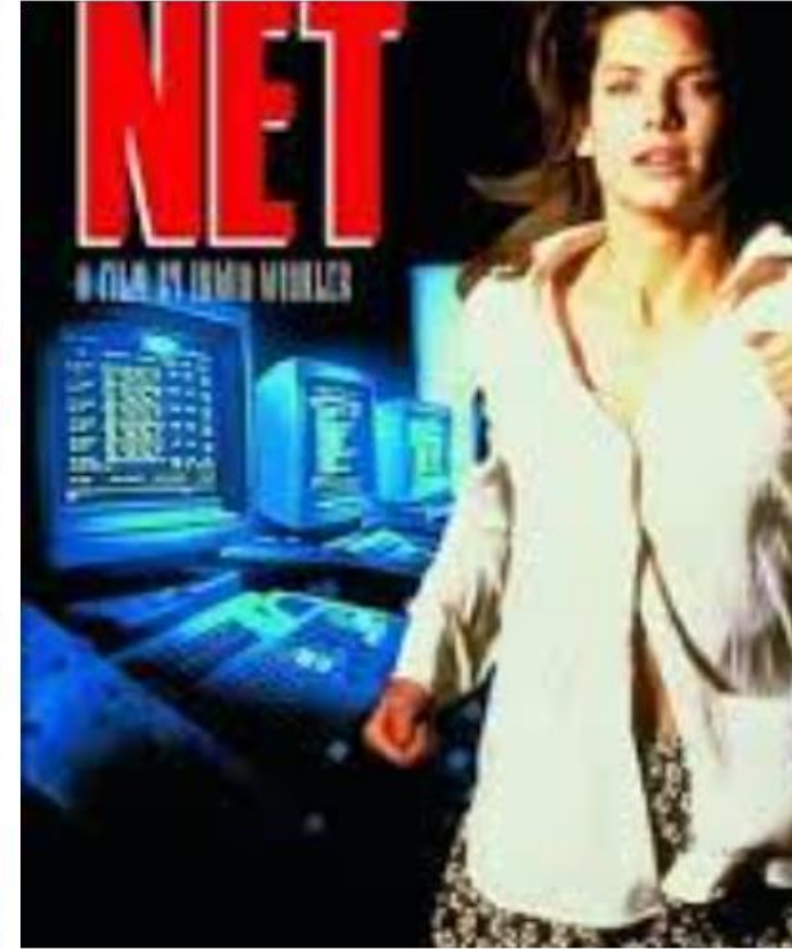
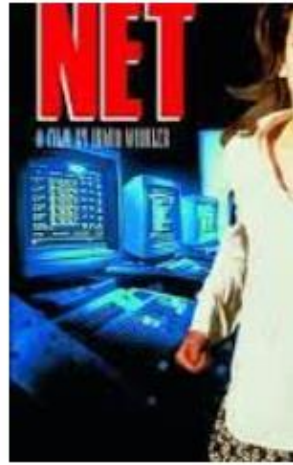
| Source                         | Target   | First call          | Last call           | Call count |
|--------------------------------|----------|---------------------|---------------------|------------|
| BAPI_USER_GET_DETAIL           |          |                     |                     |            |
| AED                            | 7793_TES | 03.02.2023 17:56:30 | 03.02.2023 17:56:30 | 1          |
| Direction: Outbound            |          |                     |                     |            |
| RFC Destination: AE3           |          |                     |                     |            |
| RFC User: TRACEADM             |          |                     |                     |            |
| Trigger User: YANKANZ          |          |                     |                     |            |
| SNC: Disabled                  |          |                     |                     |            |
| Trusted: No                    |          |                     |                     |            |
| Tier information: Tier Unknown |          |                     |                     |            |
| Create Filter                  |          |                     |                     |            |
| AED                            | 7793_TES | 03.02.2023 17:56:30 | 03.02.2023 17:56:30 | 1          |
| Direction: Outbound            |          |                     |                     |            |
| RFC Destination: AEQ           |          |                     |                     |            |
| RFC User: TRACEADM             |          |                     |                     |            |



---

# Lonza's SAP Cybersecurity Journey

# Interested in Cybersecurity ?





# Depth and Breadth

---

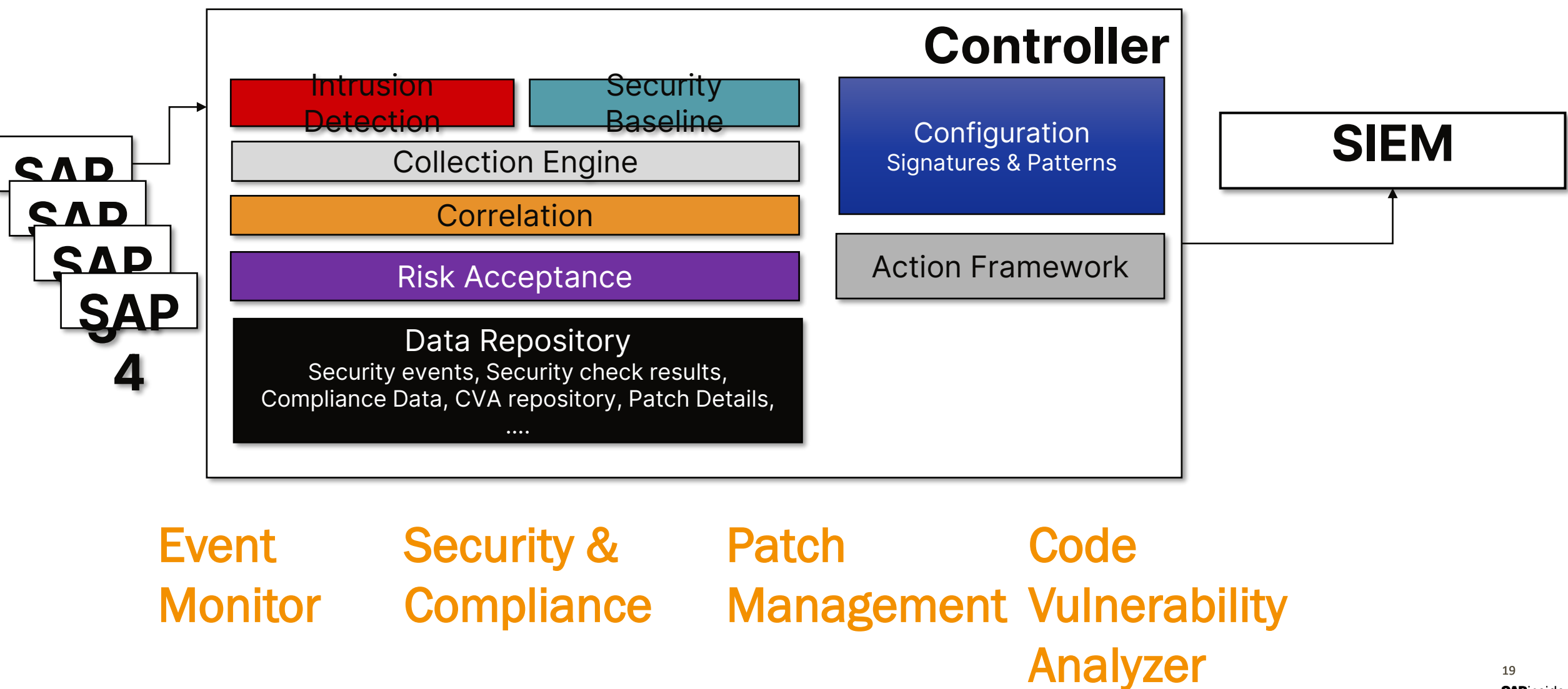
*Cybersecurity*

*Identity and Access Management*

*Data Protection and Privacy*

*Risk and Compliance*

# Implementation at Lonza



# Implementation Challenges

---

## **Sync with system owners**

Identifying critical data, obsolete clients, automated processes.

## **Low disk space**

SAP Security Audit logs consume disk space.

## **Flooding SIEM solution**

Approx. 10,000+ events recorded per day.

## **Remediation of vulnerable ABAP code**

Multiple lines of vulnerable ABAP code.

Testing ABAP code changes is time consuming.

## **Remediation of vulnerable RFC connections**

Testing authorizations for RFC connections is time consuming

## **Implementing Patches & Security notes**

Involvement of multiple teams depending on security notes



## Baby Steps

---

Dave Ramsey's Financial  
University

***"Baby Steps to Financial Security"***

***What about SAP  
Cybersecurity?***

# Baby Step 1 – Know your System

---

## Inventory Tracking

- Determine complete inventory of SAP systems.
- Determine Operating System , databases, application servers associated with SAP systems.
- Determine SAP system landscape, systems and clients with critical data to prioritize risk management.

Review existing policies for data lifecycle management, risk management, disaster recovery, incident management..

Review impact of activation of the SAP security audit log including disk space with appropriate stakeholders.

## Baby Step 2 - Baselines

---

Create an SAP Security Baseline with minimum recommended security requirements for ABAP, JAVA, HANA and Cloud based SAP Systems.

Create a policy for risk assessment of vendor software or tools related to SAP.

Create a policy to validate any new SAP systems against SAP security baselines.

# Baby Step 3 – System Monitoring

---

Create a policy for Incident management for SAP.

Approach to Implement System Monitoring

## ***1st Phase - Detect Privilege escalation***

Activate listeners to determine unauthorized changes to user master data.

Activate listeners to determine unauthorized changes to system configuration.

Push security events to SIEM system for 24/7 monitoring.

## ***2nd Phase – Detect Lateral Movement***

Activate listeners to record RFC traffic for critical calls.

Create filters to reduce noise for known traffic

## ***3rd Phase - Detect data leakage***

Activate listeners to record download of critical data



## Baby Step 4 – Interface Management

---

Create a policy which includes minimum security requirements for applications which require interface to SAP.

Create a policy which includes minimum security requirements for creation of RFC users.

Determine and remediate vulnerable RFC connections.

## Baby Step 5 – Security & Compliance Management

---

Implement security configurations changes as per minimum security requirements provided in SAP Security baseline.

Implement MFA for critical transactions and Power users

Educate end users on SAP Cyber hygiene and fraud prevention

## Baby Step 6 – ABAP Code Vulnerability

---

- Create a policy for data lifecycle management of ABAP code.
- Create a policy for remediation of vulnerable code.
- Provide training to developers to remediate vulnerable code
- Approach to Code Vulnerability Scan
  - Plan remediation of ABAP vulnerabilities identified using SAST tool.
  - Scan future transports for code vulnerabilities.
- Activate listeners to monitor dynamically generated programs in non-development systems.



## Baby Step 7 – Patch Management

---

Create a policy for implementation of Security patches and notes.

Approach to implement Patch Management

### ***1st Phase – Identification***

Review status of implementation of SAP patches & security notes.

### ***2nd Phase – Remediation***

Setup monthly meetings to review and implement SAP security notes

Develop remediation plan to patch SAP systems.

# Where to Find More Information

---

<https://www.securityweek.com/critical-sap-vulnerability-allows-supply-chain-attacks/>

- Critical SAP Vulnerability Allows Supply Chain Attacks

<https://www.abex.io/advisory>

- SAP Security Advisories

[SAP Cybersecurity interview with ChatGPT \(sapinsider.org\)](https://www.sapinsider.org/sap-cybersecurity-interview-with-chatgpt)

<https://www.cybersecuritydive.com/news/sap-vulnerabilities-urgent-patching/618647/>

- Critical SAP Vulnerabilities spur CISA, researcher pleas for urgent patching

[Global Risks Report 2024 | World Economic Forum | World Economic Forum \(weforum.org\)](https://www.weforum.org/publications/global-risks-report-2024)

- Global Risk Report 2024 – World Economic Forum

<https://securitybridge.com/security-news/what-is-the-sap-cyber-risk-appetite/>

- What is Cyber Risk Appetite

<https://www.cpomagazine.com/cyber-security/hackers-exploit-known-sap-security-vulnerabilities-with-a-typical-cyber-attack-succeeding-in-record-time/>

- Hackers exploit SAP security vulnerabilities to bypass compliance control and commit fraud

# Key Points to Take Home

---

You are the target; bad people want in!

Hackers are getting in, and the IoT is just going to make that easier

Monitoring what's going on (you will learn more about your SAP system then you ever imagined)

Communication is key – management must understand the risk

Patch Management (Security) no more later/back burner

Custom code is a risk – you need to make sure you have it covered

You need to know where you stand – the first step is always the hardest – **BABY STEPS**



# Thank you! Any Questions?

---

Bill Oliver - bill.oliver@securitybridge.com

[https://twitter.com/\\_securitybridge](https://twitter.com/_securitybridge)

<https://de.linkedin.com/company/securitybridge>

Nipun Mahajan - nipun.mahajan@lonza.com

Please remember to  
complete your session  
evaluation.

# SAPinsider



## SAPinsider.org

PO Box 982Hampstead, NH 03841  
Copyright © 2024 Wellesley Information Services.  
All rights reserved.

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. Wellesley Information Services is neither owned nor controlled by SAP SE.

---

**SAPinsider  
comprises the  
largest and fastest  
growing SAP  
membership group  
with more than  
800,000 members  
worldwide.**

---