

# The four pillars of SAP Cybersecurity

**Bill Oliver**  
**SecurityBridge Inc.**  
**ASUG New England 2024**



# Agenda

- SAP Security Surroundings
- The 4 Pillars
- Hardening your SAP Security Position
- Security Patch Management
- Custom Code Vulnerabilities
- Security Monitoring

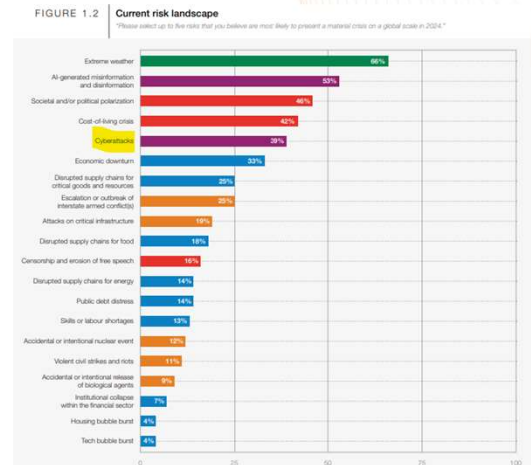
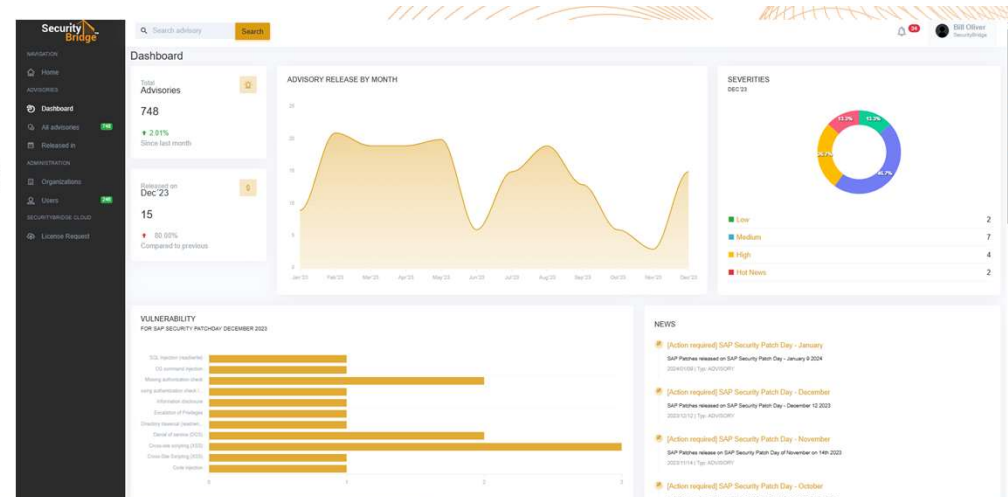


# SAP Security Surroundings

## 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>



## ATTACK VECTORS

**VULNERABILITY  
MANAGEMENT**

**CONFIGURATION  
VULNERABILITY**

**PATCH  
MANAGEMENT**

**KNOWN PRODUCT  
ERROR**

**CODE  
SCANNER**

**CUSTOMER CODE  
VULNERABILITY**

**THREAT  
DETECTION**

**ZERO  
DAY**



1010  
1010



# Hardening your SAP Security Position



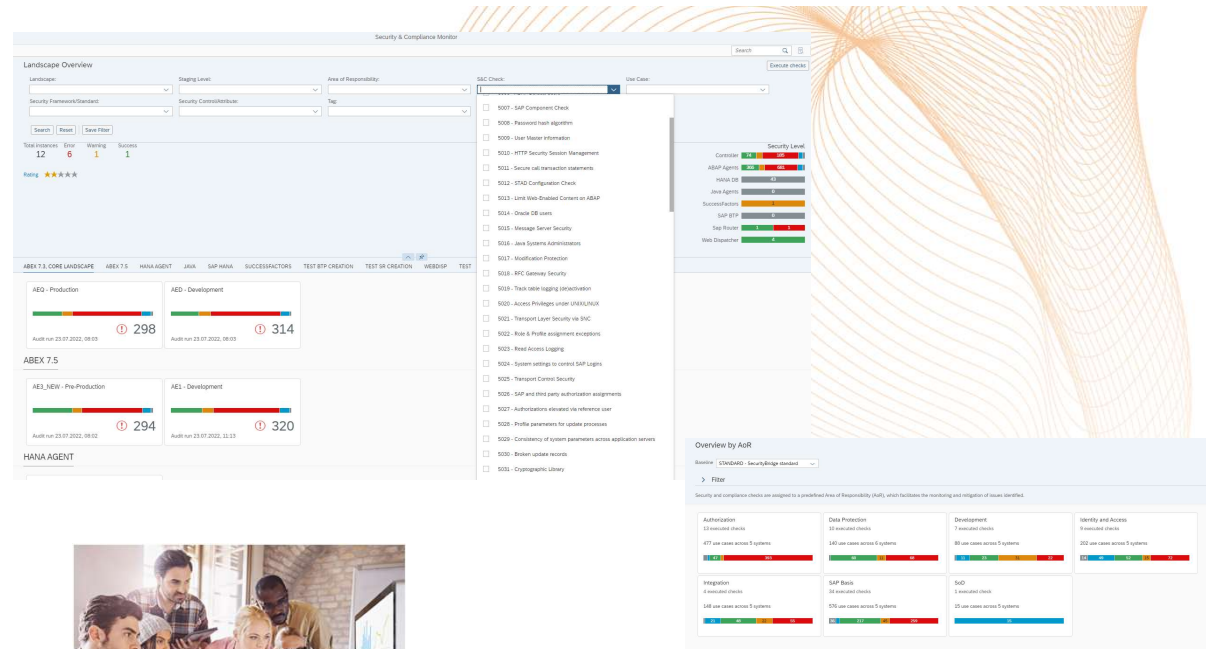


# Hardening your SAP Security Position

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 (PCFG), 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 - 2023-05-21  
**SAP HANA Security Guide for SAP HANA Platform**

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

CUSTOMER/PARTNER



© All rights reserved SecurityBridge GmbH 2024 | PUBLIC

THE BEST RUN 

 Run Simple

# Security Patch Management



# SAP Security Patch Management

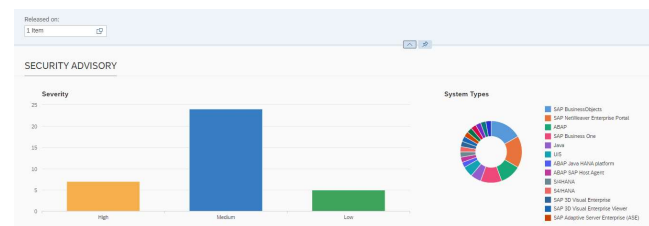
For those who don't know, SAP has what we call "Patch Tuesday." On the second Tuesday of every month, SAP releases Security patches. They break them up into four categories: Hot News, High, Medium, and Low.

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

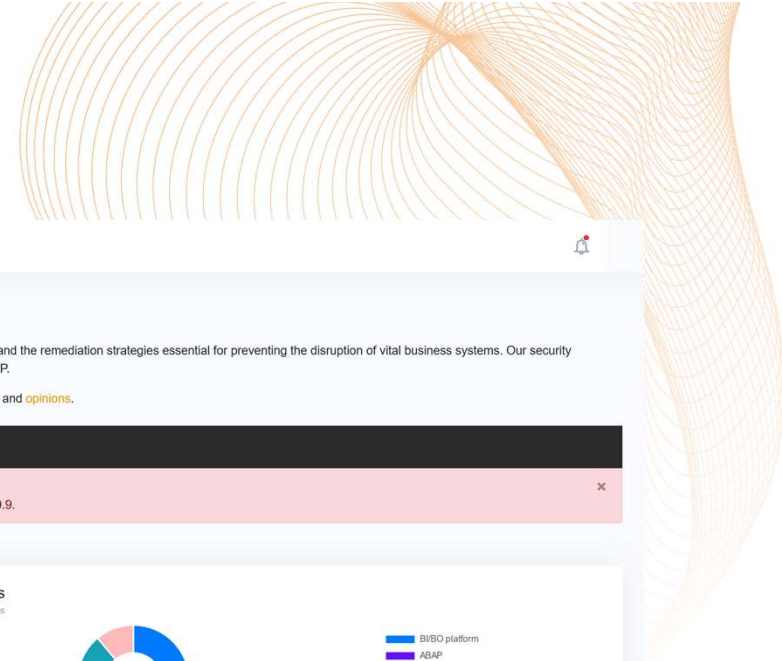
Month	Planned Date
January	30
February	14
March	14
April	13
May	9
June	13
July	11
August	8





# Security Advisories

[Cloud.SecurityBridge.com](https://cloud.securitybridge.com)



The screenshot shows the SecurityBridge Cloud Platform interface for Security Advisories. It features a dark sidebar with navigation options: Home, Dashboard, All advisories (590), and Released in. The main content area includes a search bar, a title 'Security Advisories', and an introductory paragraph. A 'Patchdays' filter is set to 2023. A notification banner states: 'Yikes, there is work to do! This time we found critical correction advisories. We count 9 and the highest CVSS score is 9.9.' Below this are two charts: 'Severity' (a bar chart showing 9 advisories with scores ranging from 4.0 to 5.0) and 'System Types' (a donut chart showing the distribution of affected SAP system types). At the bottom, three advisory cards are displayed, each with a CVSS score of 9.9 or 9.4 and a release date of 2023-01-10.

Severity	Count
Low	0
Medium	9
High	0
Hot News	0

System Type	Count
BI/BO platform	1
ABAP	1
Java	1
Kernel / ABAP	1
SAP Business Planning and Consolidation	1
SAP Host Agent	1

Related note	CVSS	Severity
3275391	9.9	High
3262810	9.9	High
3268093	9.4	High



# Custom Code Vulnerabilities



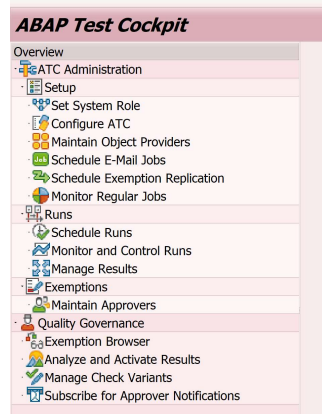
# Custom Code Vulnerabilities

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

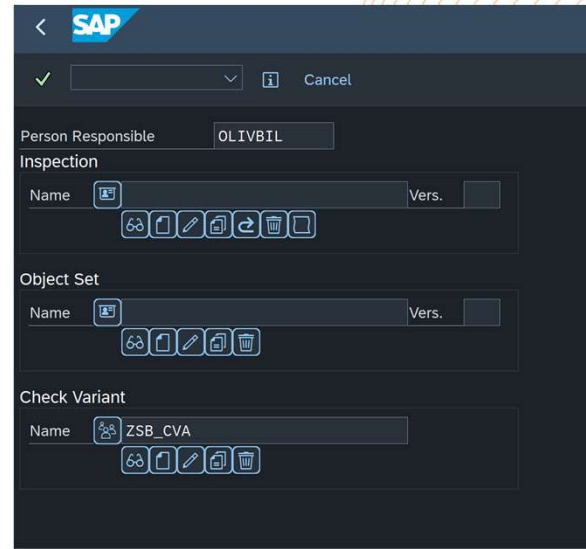
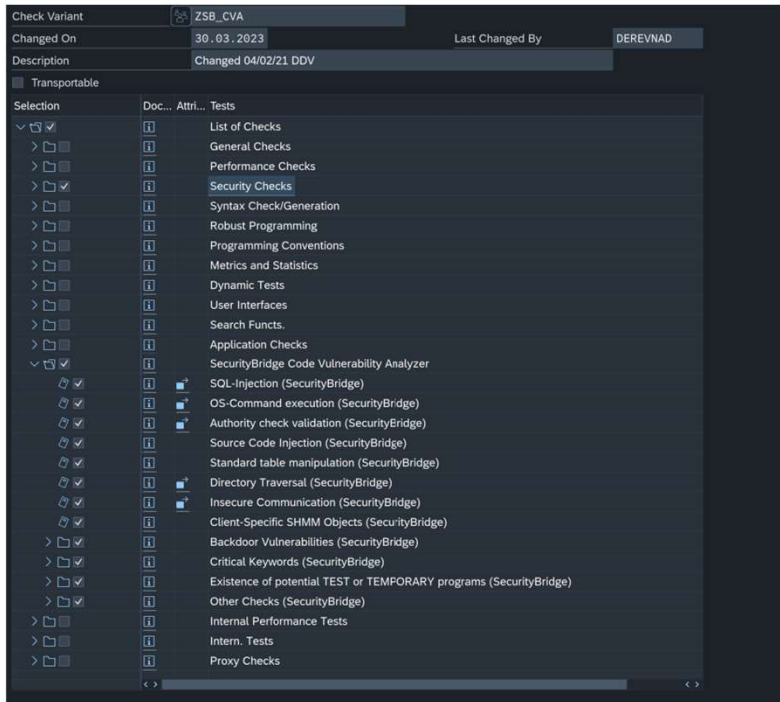
- Overview
  - ATC Administration
    - Setup
      - Set System Role
      - Configure ATC
      - Maintain Object Providers
      - Schedule E-Mail Jobs
      - Schedule Exemption Replication
      - Monitor Regular Jobs
    - Runs
      - Schedule Runs
      - Monitor and Control Runs
      - Manage 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

Check Name	Error	Warning	Information
List of Checks	13	1	0
Performance Checks	0	1	0
Security Checks	0	0	0
Critical Statements	0	0	0
System Check/Conversion	0	0	0
Robust Programming	0	0	0
User Interfaces	0	0	0
SecurityBridge Code Vulnerability Analyzer	0	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 generic TFC or TFCHECK programs (SecurityBridge)	1	0	0
Client Specific Shared Object Methods (SecurityBridge)	1	0	0
Other Checks (SecurityBridge)	1	0	0



# ATC integration



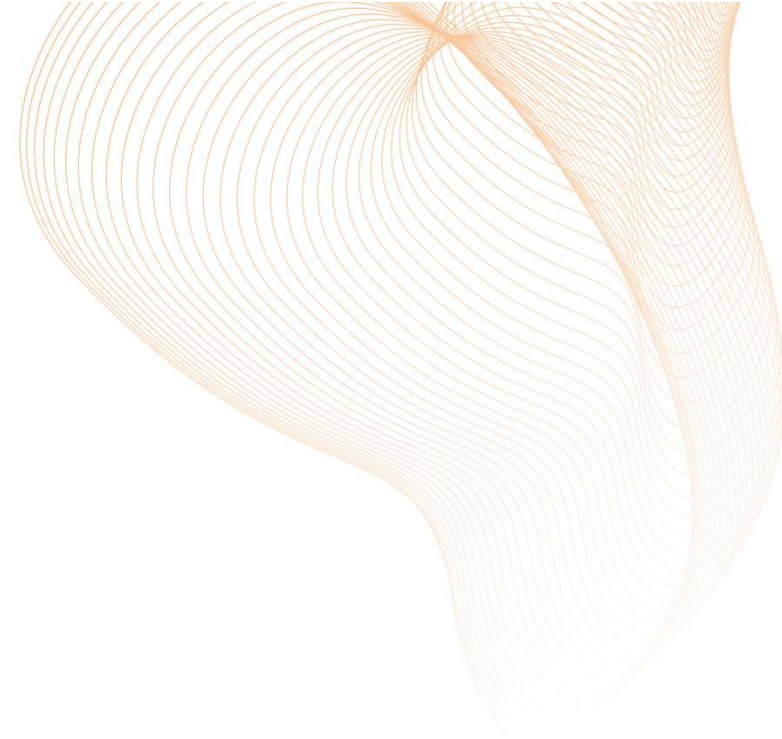
The screenshot shows the results screen for 'ATC: ZGETHASH' in SAP SecurityBridge. It features a table with columns for 'Pri.', 'Check Title', 'Check Message', 'Object Name', 'Obj.', and 'Ex.'. The table contains five rows of findings.

Pri.	Check Title	Check Message	Object Name	Obj.	Ex.
1	Authority check validation (SecurityBridge)	Missing authority-check for executable program	ZGETHASH	PROG	
1	Authority check validation (SecurityBridge)	No authorization group assigned to the executable	ZGETHASH	PROG	
1	Executable program without transaction code (SecurityBridge)	No transaction code assigned to the executable pr	ZGETHASH	PROG	
1	Backdoor identification on user (SecurityBridge)	Possible conditional check on User Name ... ..	ZGETHASH	PROG	
1	Access to password hashes (SecurityBridge)	Access to password hash values via ... (through S	ZGETHASH	PROG	





# 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

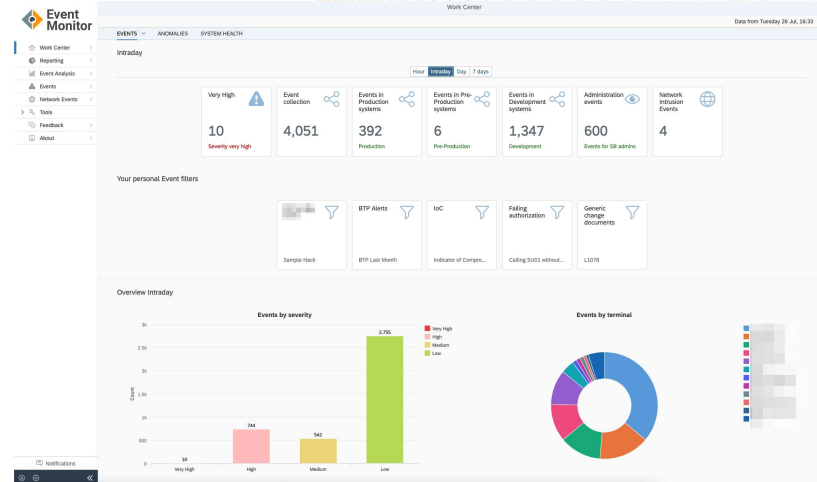
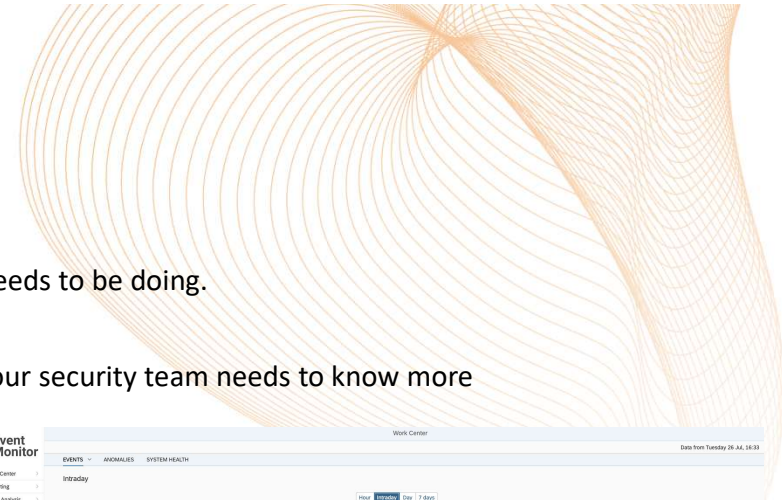
Analysis of Security Audit Log

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

Audit Classes	Dialog Logon	RFC/DIRC/Logon	RFC Function Call	Transaction Start	Report Start	User Master Change	Other Events	System Events
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: Active status set to 1		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: configuration changed		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: Slot 1 Inactive		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: Slot 2 Inactive		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: configuration changed		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: Slot 1 Inactive		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: configuration changed		
04.01.2019 21:28:05	600	BOLVER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: configuration changed		
04.01.2019 21:34:52	600	HACKER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: configuration changed		
04.01.2019 21:34:52	600	HACKER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: Slot 1, Class 64, Severity 2, User "", Client "",		
04.01.2019 21:34:52	600	HACKER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: configuration changed		
04.01.2019 21:34:52	600	HACKER	DESKTOP-D09HDD	SM19	SAPMSH19	Audit: Slot 2 Inactive		

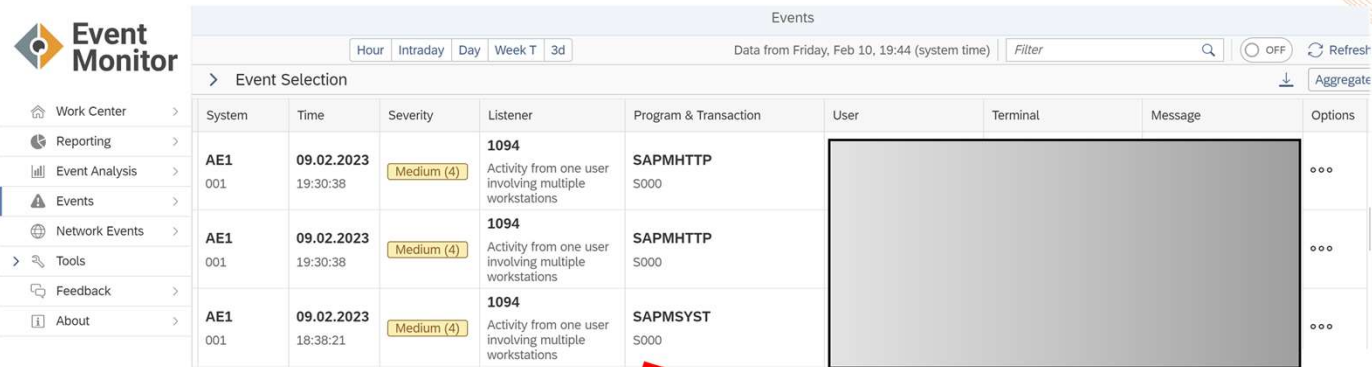


Security Guide | INTERNAL - Authorized for SAP Customers and Partners  
 SAP Enterprise Threat Detection  
 2024-03-09  
**Security Guide for SAP Enterprise Threat Detection**  
 Release 2.0, Support Package 6



# Now what ?

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



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:

Description:

\*Action Type:

\*Action timing:  Send an email

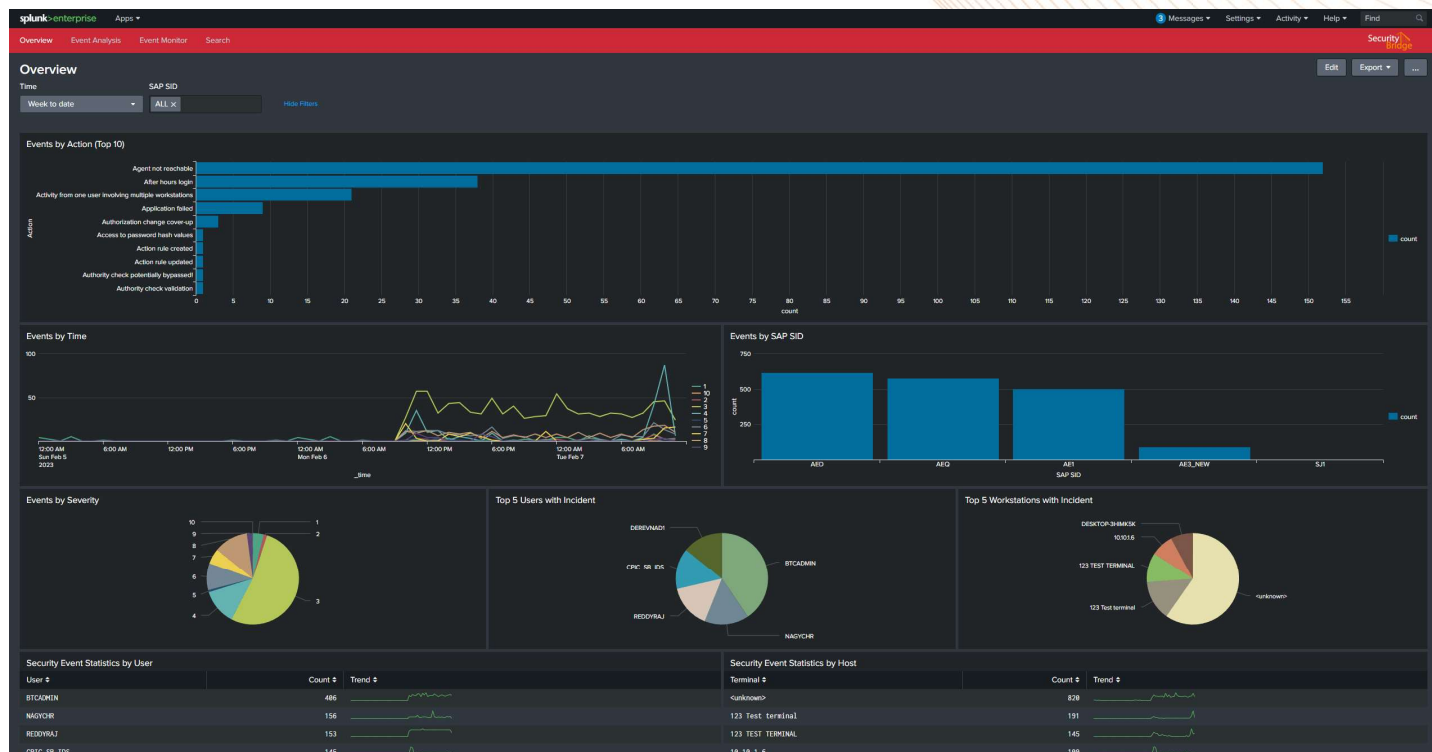
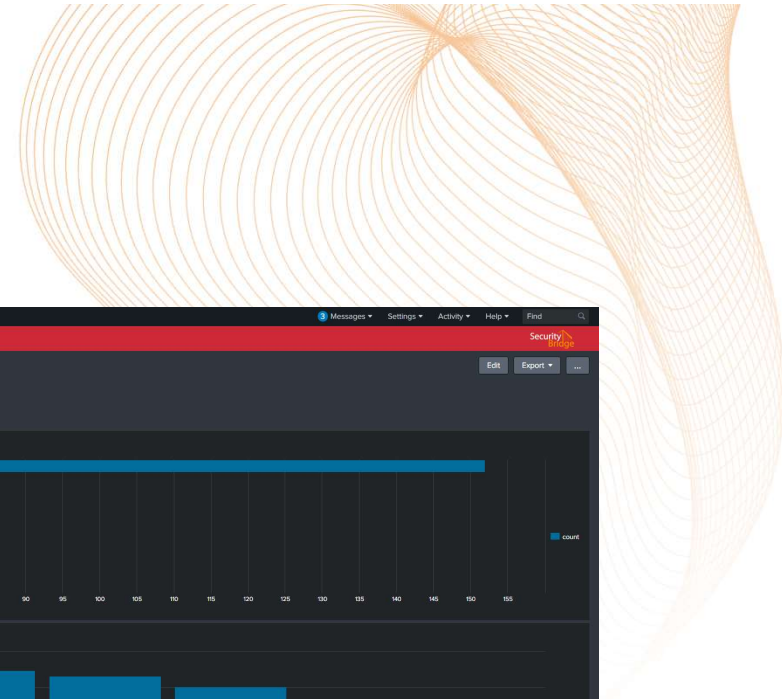
\*Valid from:  Show a popup to the user triggering the event

\*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



# SIEM tools



# 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

**RFC destinations in use**

26

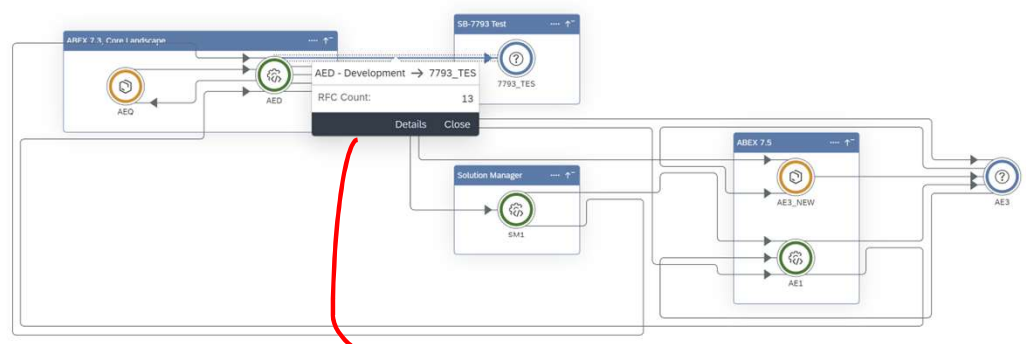
**Security relevant RFC calls**

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

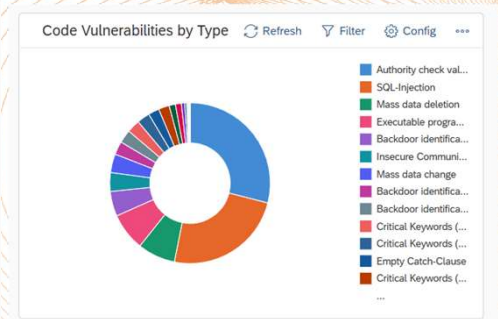
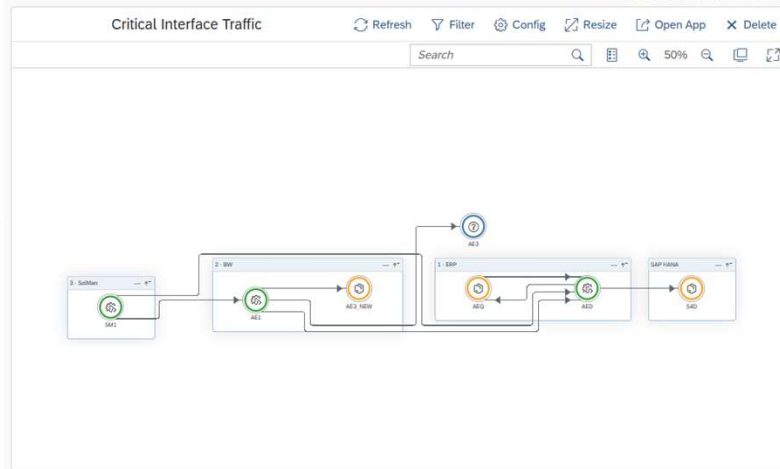
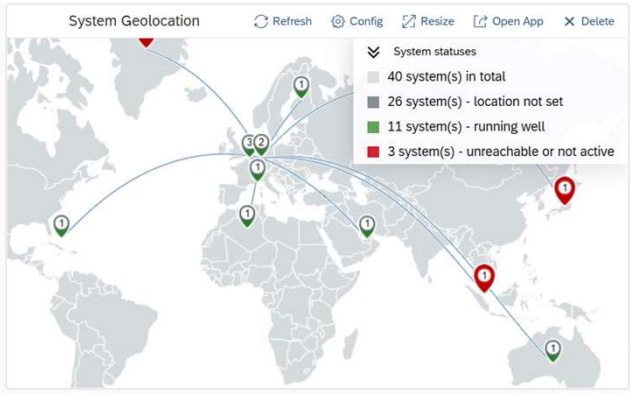
RFC traffic statistics (5)

Source	Target	First call	Last call	Call count
<b>BAPI_USER_GET_DETAIL</b>				
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				
<a href="#">Create Filter</a>				
AED	7793_TES	03.02.2023 17:56:30	03.02.2023 17:56:30	1
Direction: Outbound				
RFC Destination: AEQ				
RFC User: TRACEADM				



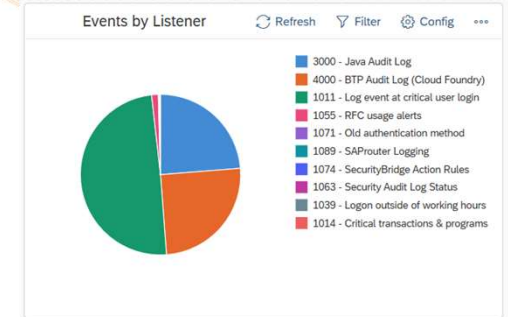
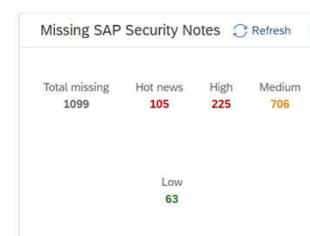


# Dashboard (tie it all together)



**Interface Security**

RFC Recorder No. of systems	Critical access paths (used)
5 active 1 not active	6
RFC destinations in use	Security relevant RFC calls
9	605,518



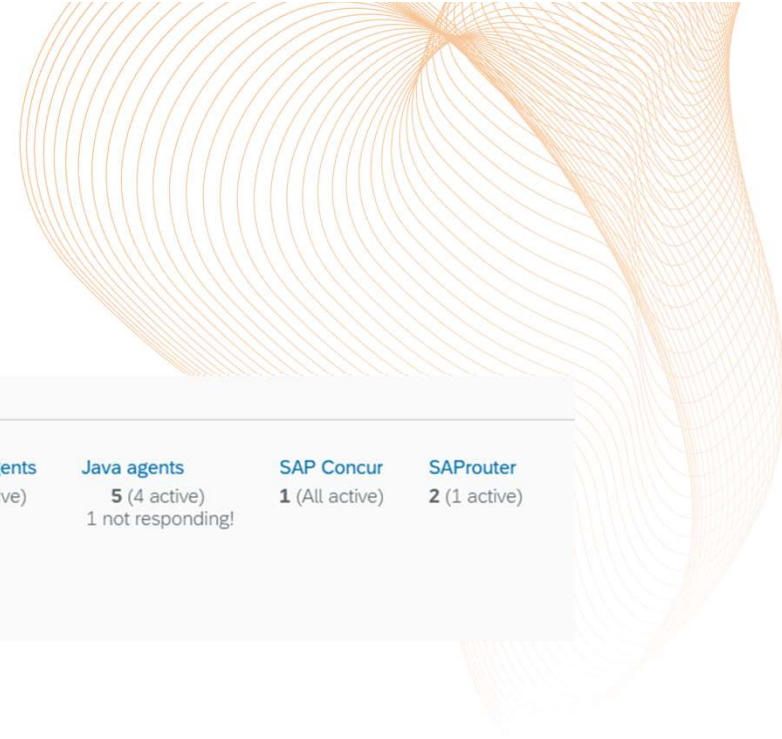
**Top 5 Impact Issues**

Use Case	Exploitation risk	Resolution Complexity	System	Status	Description of Status
<b>U5016_0001</b> Java Systems Administrators critical roles	Very High	Medium	AED	✗	7 out of 275 user accounts have critical authorization rights.
			SM1	✗	31 out of 101 user accounts have critical authorization rights.
<b>U6012_0001</b> Password DTR Emergency User	Very High	Medium	J75	✗	Either no emergency user is maintained or the password is not maintained in the property file.
			SJ1	✗	Either no emergency user is maintained or the password is not maintained in the property file.



# Everything is at risk

---



## Summary

<b>Total systems</b> 40 (30 active) 4 not responding!	<b>ABAP agents</b> 6 (All active)	<b>BTP Global Account</b> 2 (All active)	<b>BTP Subaccount</b> 5 (All active) 1 not responding!	<b>CloudConnector</b> 2 (1 active)	<b>FortiGate</b> 2 (1 active)	<b>HANA agents</b> 5 (4 active)	<b>Java agents</b> 5 (4 active) 1 not responding!	<b>SAP Concur</b> 1 (All active)	<b>SAProuter</b> 2 (1 active)
<b>SuccessFactors</b> 4 (1 active)	<b>S/4HANA Public Cloud</b> 2 (1 active)	<b>WebDispatcher</b> 3 (2 active) 2 not responding!	<b>SAP BO</b> 1 (All active)						

***Include DEV, QA, PRD, etc.....***



## Takeaway

---

**You are the target; bad people want in!**

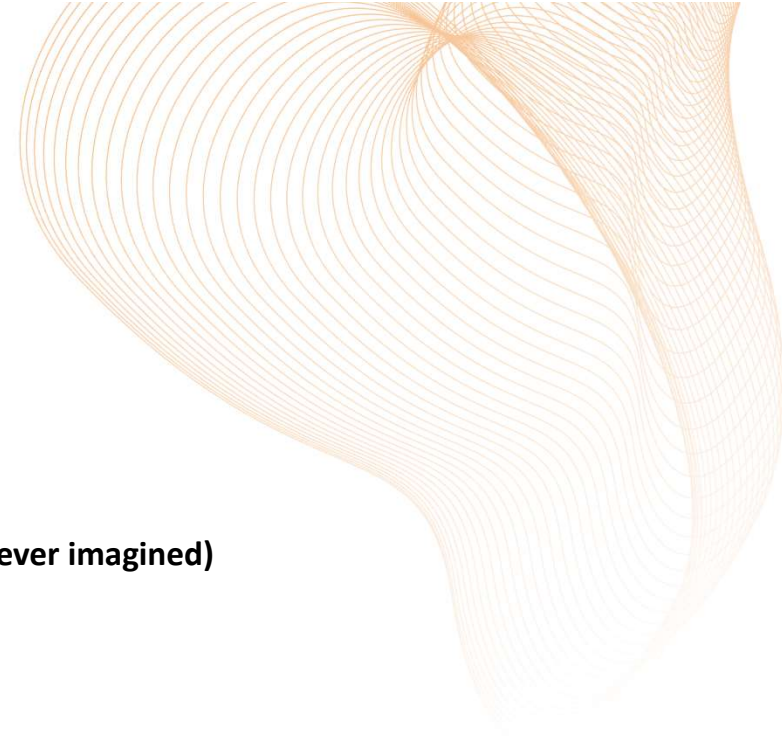
**Hackers are getting in, and the IoT is just going to make that easier**

**Monitoring what's going on (you will learn more about your SAP system than 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**





# GET IN TOUCH WITH US

 [www.securitybridge.com](http://www.securitybridge.com)

 USA: 228 Park Ave S, PMB 89765, New York, New York 10003-1502 US

 USA: +1 (416) 821 0850

 [linkedin.com/company/securitybridge](https://linkedin.com/company/securitybridge)

 SecurityBridge

 @\_SecurityBridge

