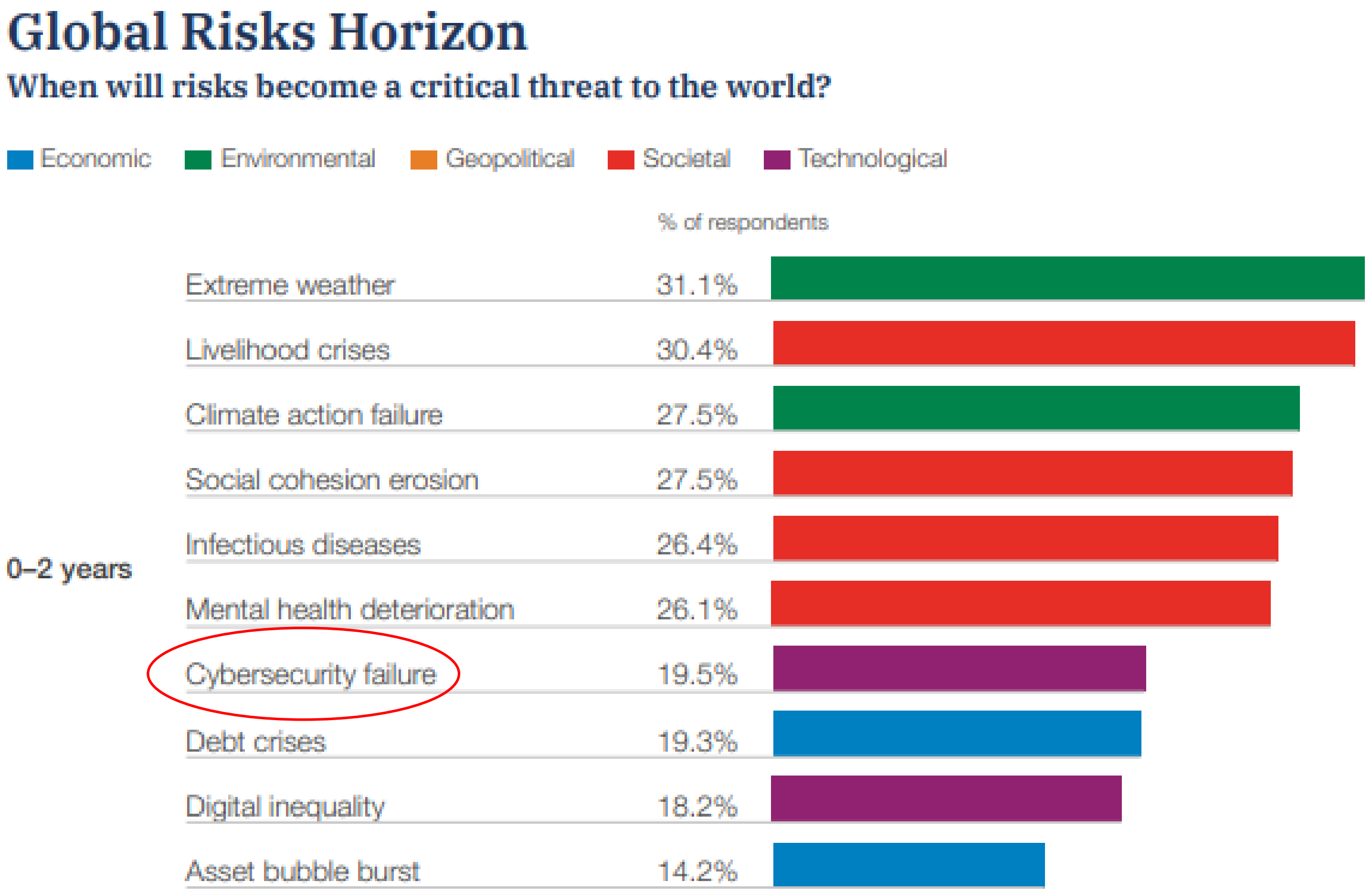
SAP Cybersecurity
How does it work?

Northern California ASUG, August 3 2022

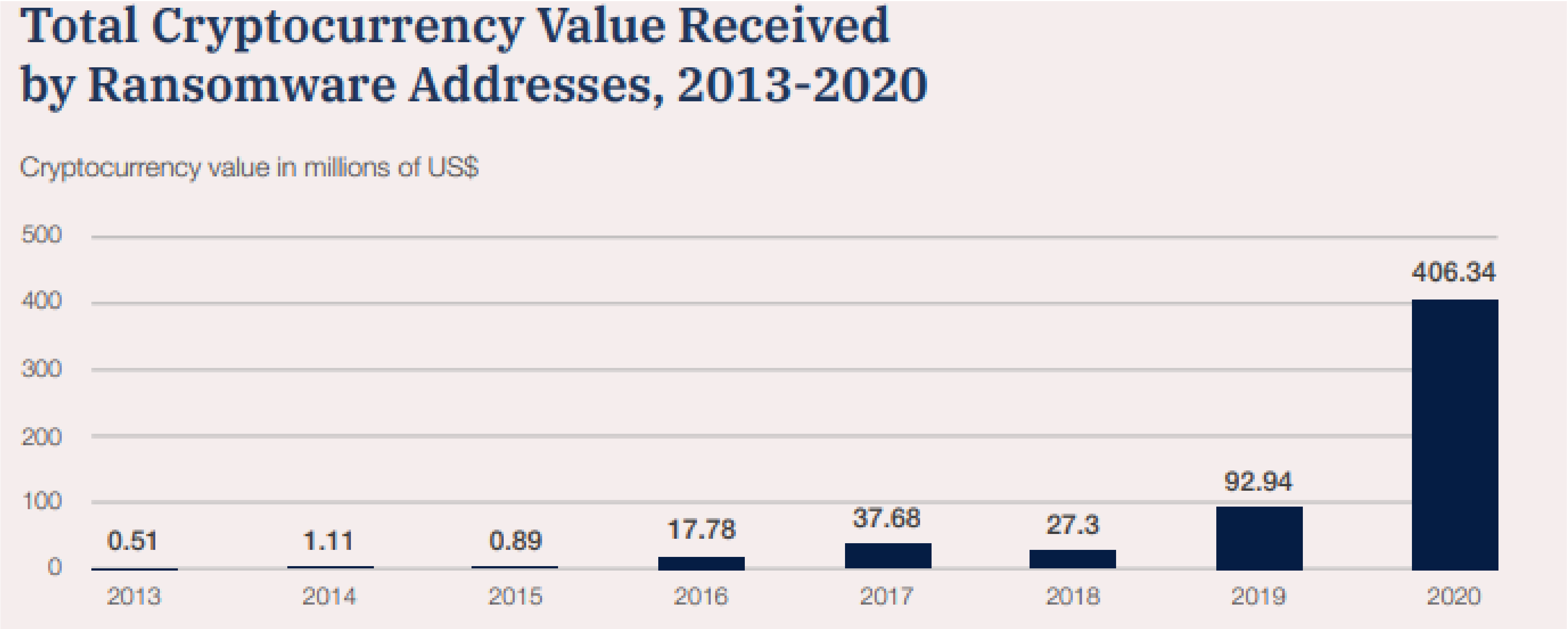
SecurityBridge™

A little overview



Global Risks Horizon

When will risks become a critical threat to the world?



Total Cryptocurrency Value Received by Ransomware Addresses, 2013-2020

Source: Global Risk Report 2022 – World Economic Forum

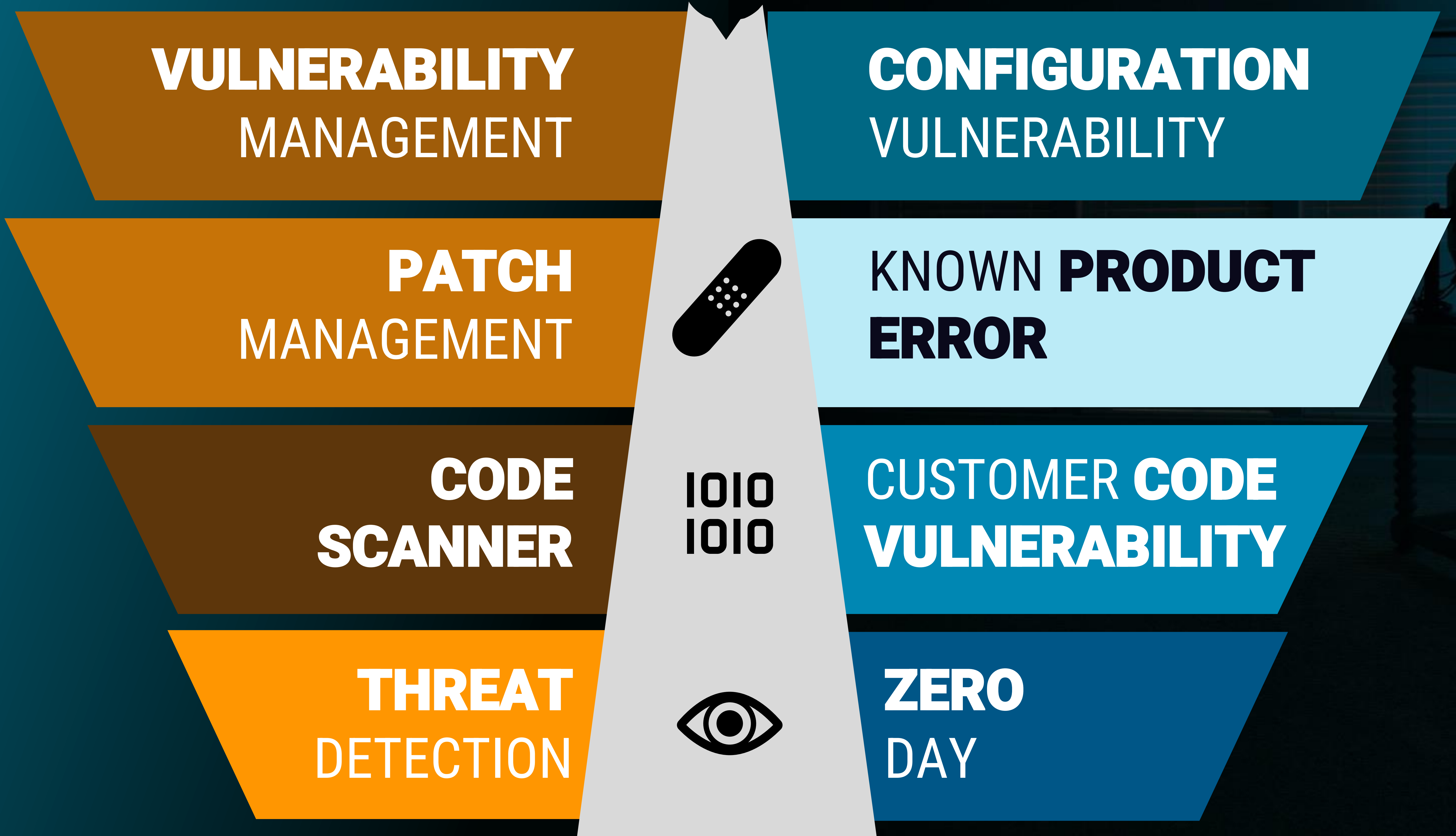
why
SAP Security

- Between mid 2020 and March 2021, 3 out of every 15 cyber attacks were successful in exploiting target SAP systems.*
- While IT teams focus security on networking, hardware, etc, the SAP application itself is often overlooked.

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

Security Bridge™

ATTACK VECTORS



VULNERABILITY MANAGEMENT

PATCH MANAGEMENT

CODE SCANNER

THREAT DETECTION

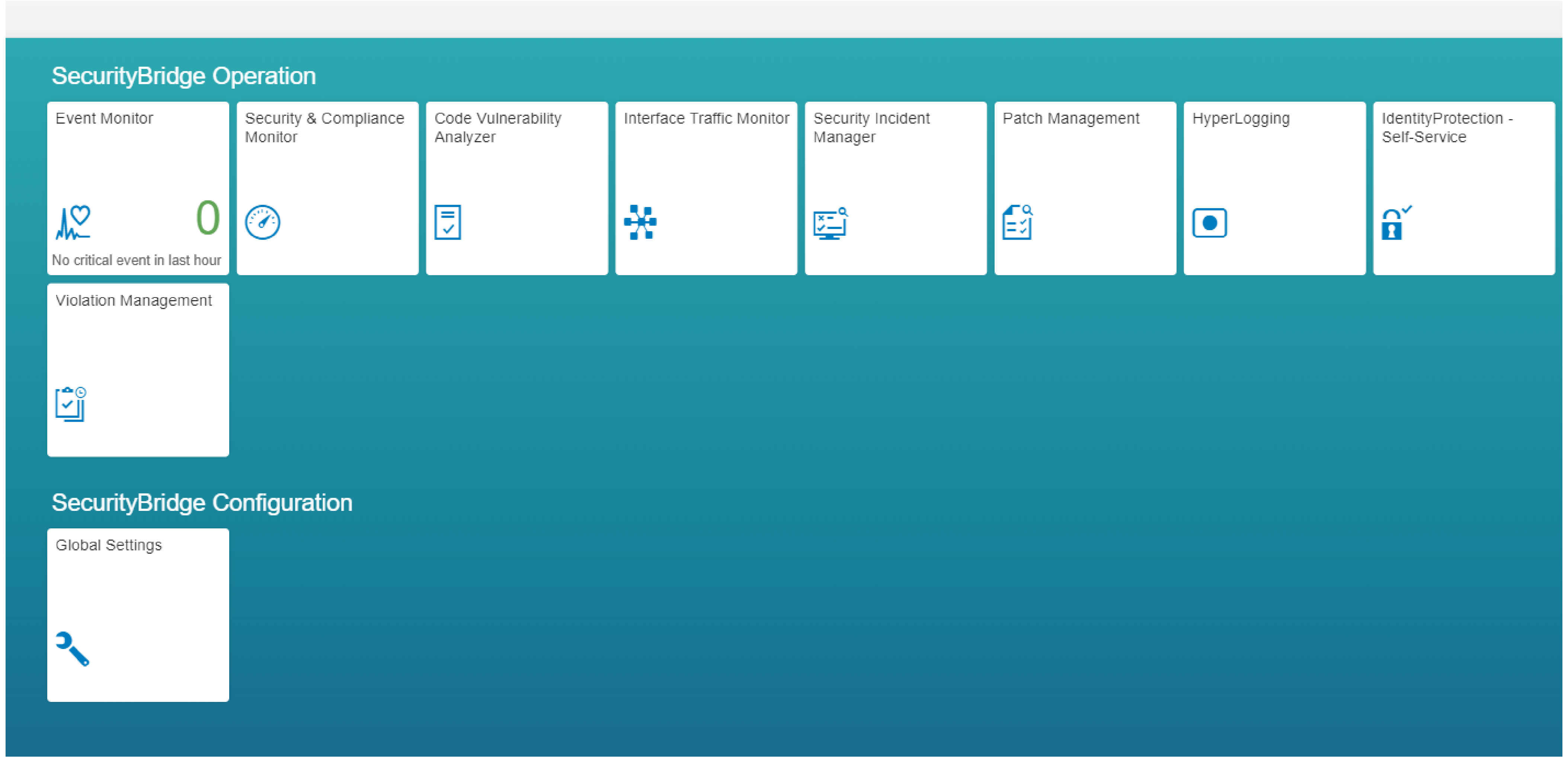
CONFIGURATION VULNERABILITY

KNOWN PRODUCT ERROR

CUSTOMER CODE VULNERABILITY

ZERO DAY

SAP Cybersecurity – Single Pane of Glass (Fiori, Splunk, etc.…)

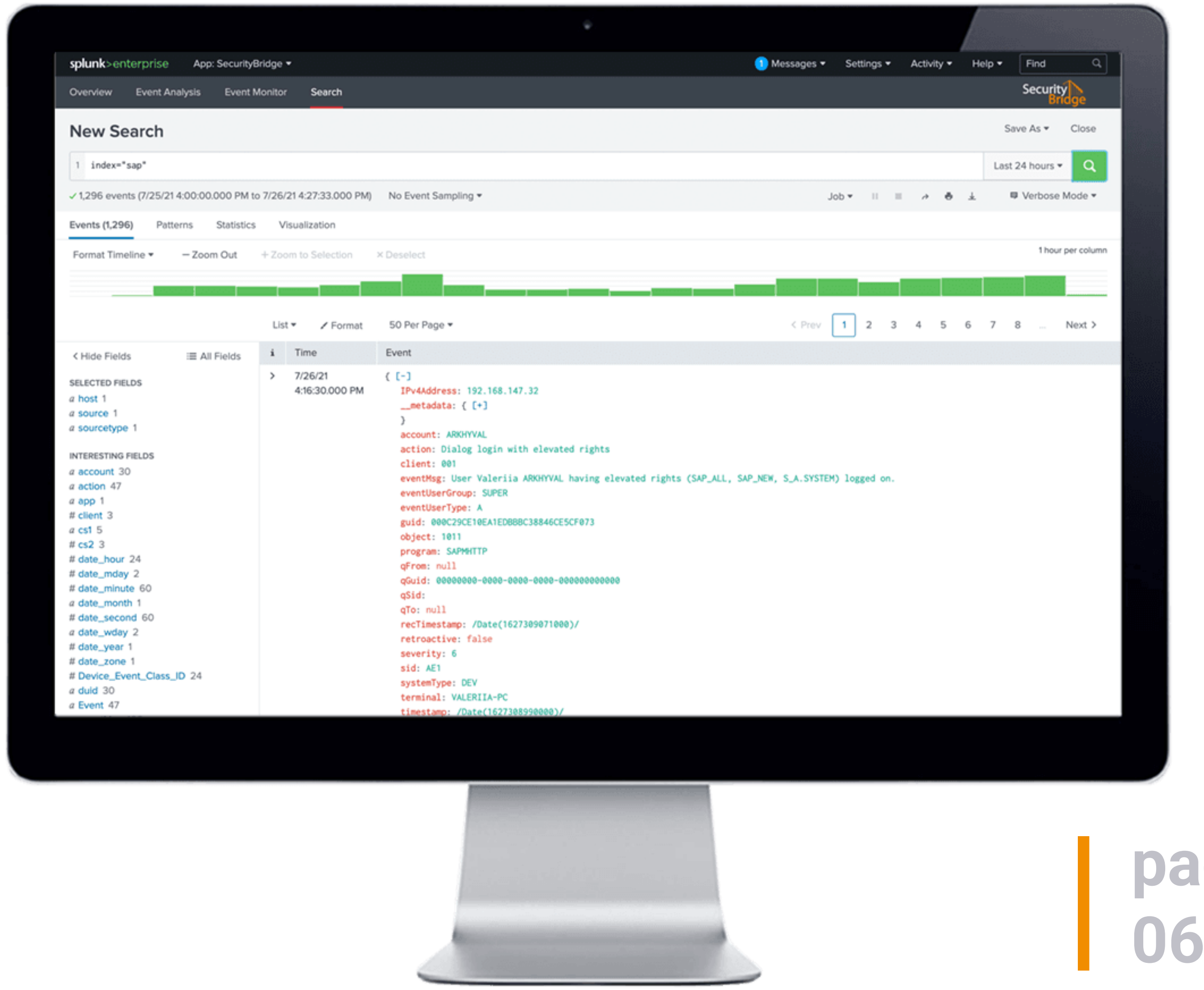


SecurityBridge Operation

- Event Monitor – 0 – No critical event in last hour
- Security & Compliance Monitor
- Code Vulnerability Analyzer
- Interface Traffic Monitor
- Security Incident Manager
- Patch Management
- HyperLogging
- IdentityProtection - Self-Service
- Violation Management

SecurityBridge Configuration

- Global Settings



New Search

```
index="sap"
```

✓ 1,296 events (7/25/21 4:00:00.000 PM to 7/26/21 4:27:33.000 PM) No Event Sampling ▾

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

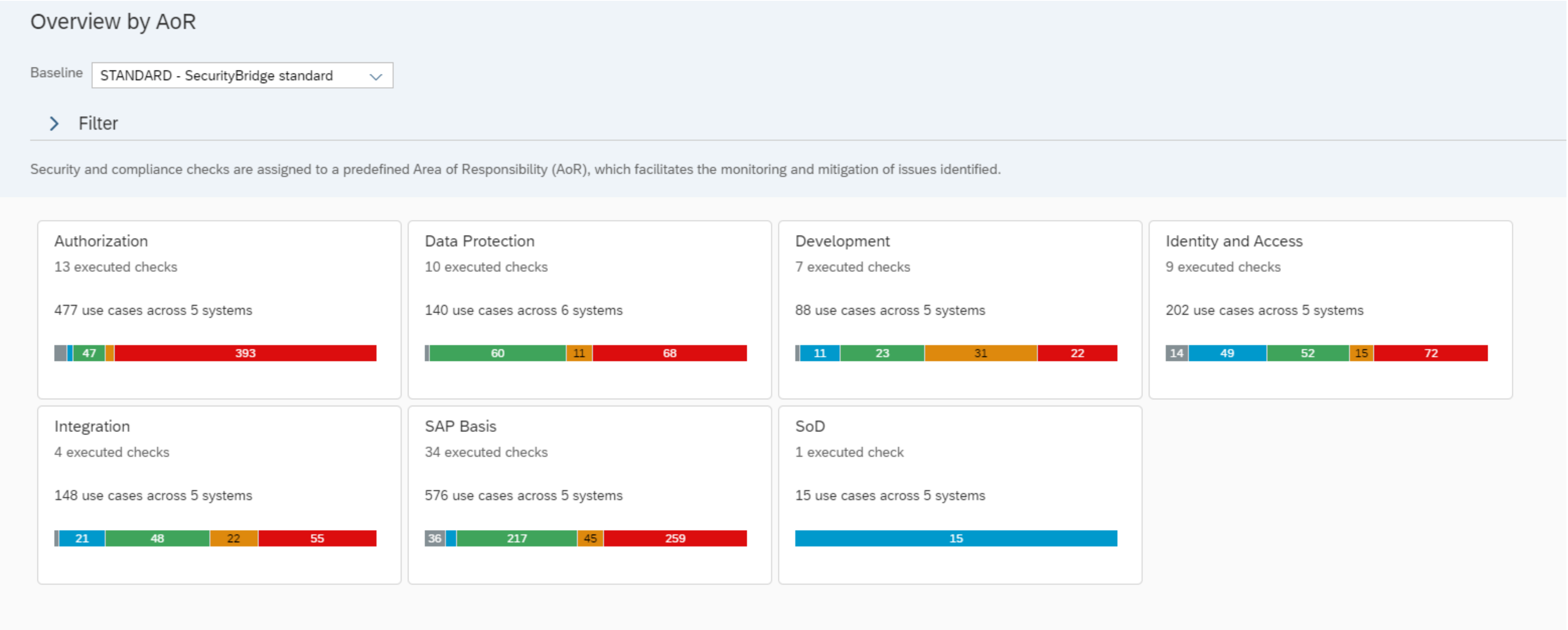
a account 30
a action 47
a app 1
# client 3
a cs1 5
# cs2 3
# date_hour 24
# date_mday 2
# date_minute 60
a date_month 1
# date_second 60
a date_wday 2
# date_year 1
# date_zone 1
Device_Event_Class_ID 24
a duid 30
a Event 47

i	Time	Event
>	7/26/21 4:16:30.000 PM	

```
{ [-]
  IPv4Address: 192.168.147.32
  __metadata: { [+]
  }
  account: ARKHYVAL
  action: Dialog login with elevated rights
  client: 001
  eventMsg: User Valeriia ARKHYVAL having elevated rights (SAP_ALL, SAP_NEW, S_A.SYSTEM) logged on.
  eventUserGroup: SUPER
  eventUserType: A
  guid: 000C29CE10EA1EDB8BC38846CE5CF073
  object: 1011
  program: SAPMHTTP
  qFrom: null
  qGuid: 00000000-0000-0000-0000-000000000000
  qSid:
  qTo: null
  recTimestamp: /Date(1627309071000)/
  retroactive: false
  severity: 6
  sid: AE1
  systemType: DEV
  terminal: VALERIIA-PC
  timestamp: /Date(1627308990000)/
```

Security and Compliance Vulnerability Management

Performing regular reviews to ensure Security configuration is correctly configured



Overview by AoR

Baseline: STANDARD - SecurityBridge standard

› Filter

Security and compliance checks are assigned to a predefined Area of Responsibility (AoR), which facilitates the monitoring and mitigation of issues identified.

Authorization
13 executed checks
477 use cases across 5 systems

Data Protection
10 executed checks
140 use cases across 6 systems

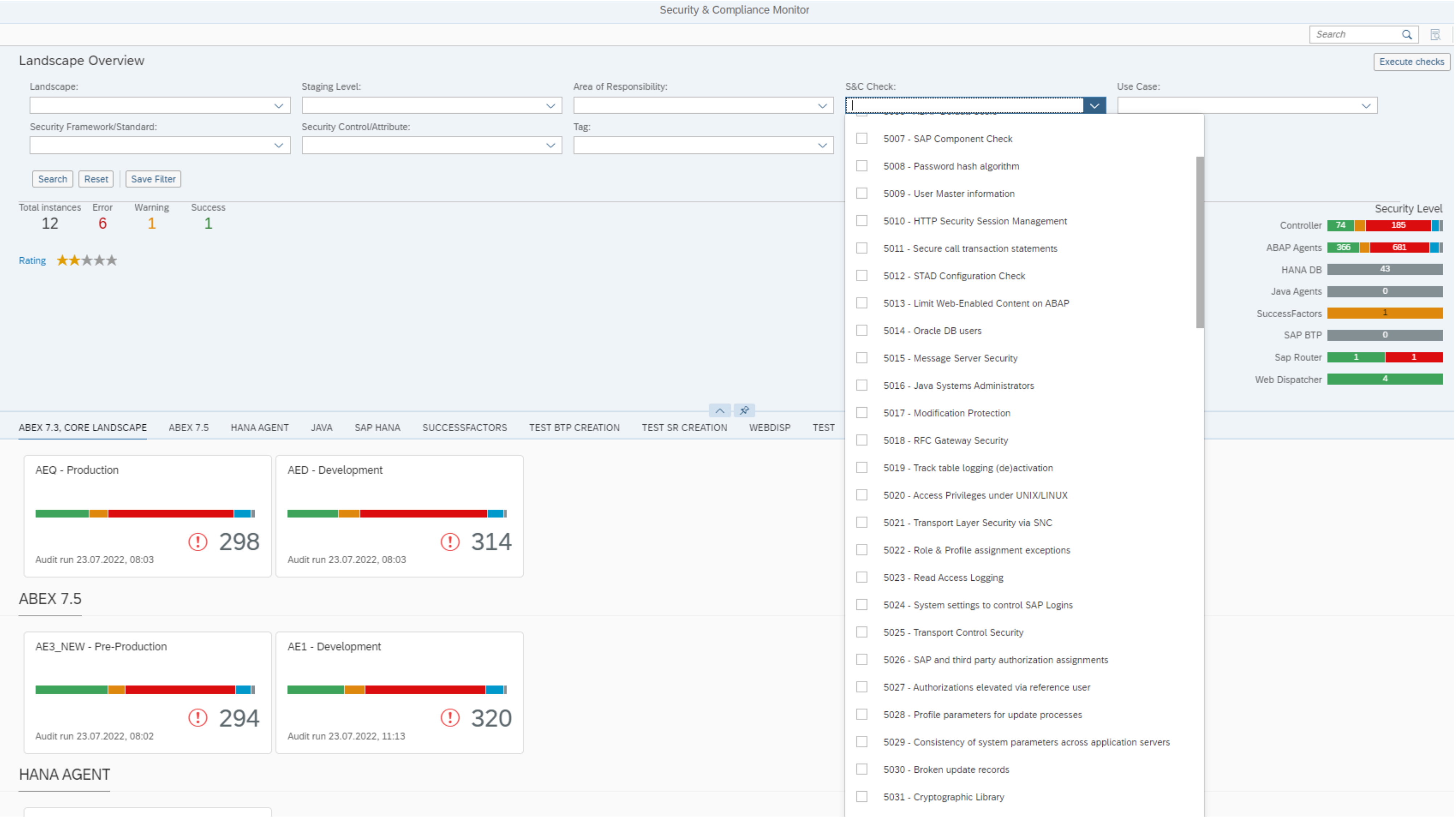
Development
7 executed checks
88 use cases across 5 systems

Identity and Access
9 executed checks
202 use cases across 5 systems

Integration
4 executed checks
148 use cases across 5 systems

SAP Basis
34 executed checks
576 use cases across 5 systems

SoD
1 executed check
15 use cases across 5 systems



Security & Compliance Monitor

Landscape Overview

Landscape:

Staging Level:

Area of Responsibility:

S&C Check:

Use Case:

Security Framework/Standard:

Security Control/Attribute:

Tag:

Total instances	Error	Warning	Success
12	6	1	1

Rating ★★★★★

- □ 5007 - SAP Component Check
- □ 5008 - Password hash algorithm
- □ 5009 - User Master information
- □ 5010 - HTTP Security Session Management
- □ 5011 - Secure call transaction statements
- □ 5012 - STAD Configuration Check
- □ 5013 - Limit Web-Enabled Content on ABAP
- □ 5014 - Oracle DB users
- □ 5015 - Message Server Security
- □ 5016 - Java Systems Administrators
- □ 5017 - Modification Protection
- □ 5018 - RFC Gateway Security
- □ 5019 - Track table logging (de)activation
- □ 5020 - Access Privileges under UNIX/LINUX
- □ 5021 - Transport Layer Security via SNC
- □ 5022 - Role & Profile assignment exceptions
- □ 5023 - Read Access Logging
- □ 5024 - System settings to control SAP Logins
- □ 5025 - Transport Control Security
- □ 5026 - SAP and third party authorization assignments
- □ 5027 - Authorizations elevated via reference user
- □ 5028 - Profile parameters for update processes
- □ 5029 - Consistency of system parameters across application servers
- □ 5030 - Broken update records
- □ 5031 - Cryptographic Library

Security Level

Controller	74 185
ABAP Agents	366 681
HANA DB	43
Java Agents	0
SuccessFactors	1
SAP BTP	0
Sap Router	1 1
Web Dispatcher	4

ABEX 7.3, CORE LANDSCAPE

AEQ - Production
298
Audit run 23.07.2022, 08:03

AED - Development
314
Audit run 23.07.2022, 08:03

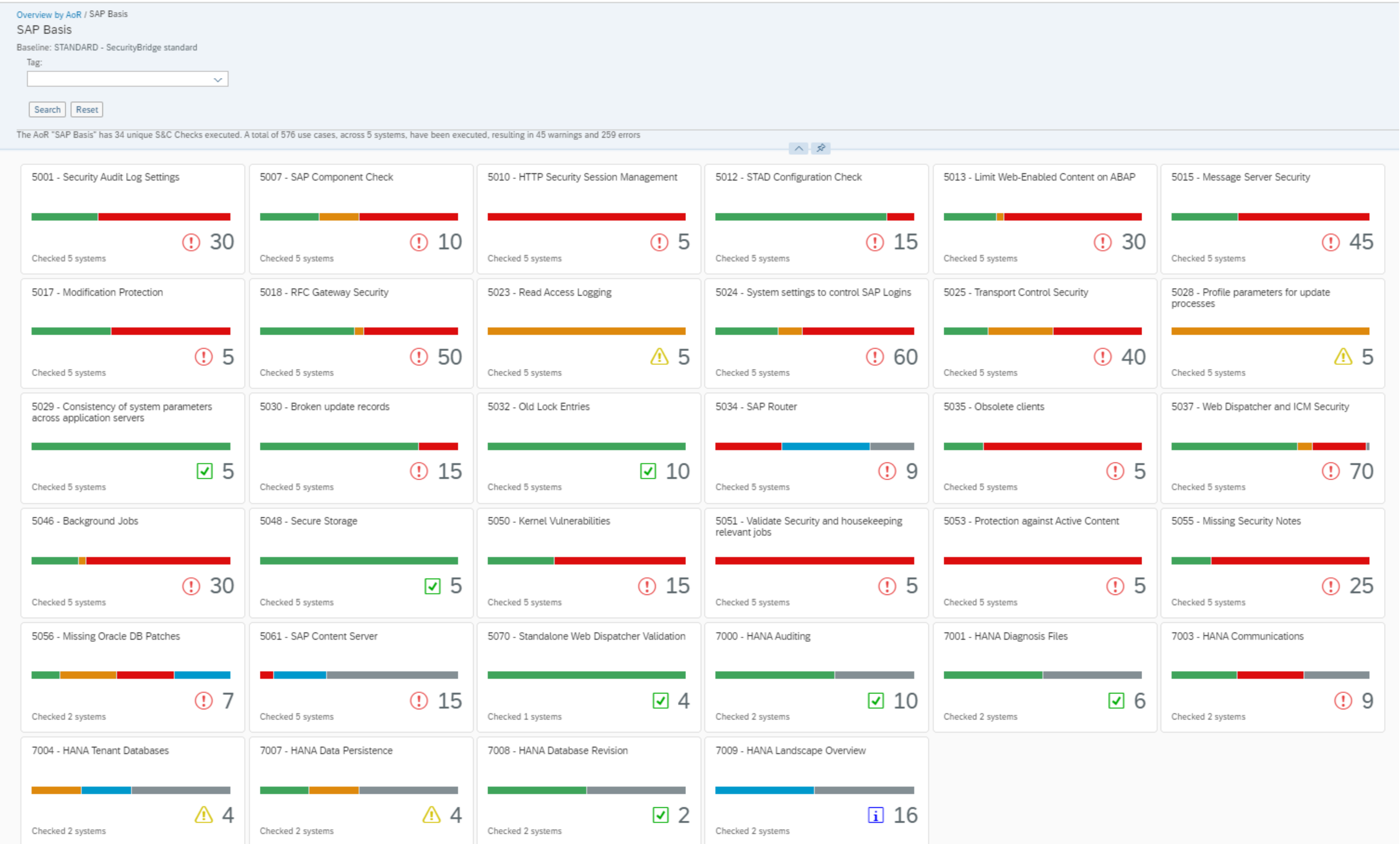
ABEX 7.5

AE3_NEW - Pre-Production
294
Audit run 23.07.2022, 08:02

AE1 - Development
320
Audit run 23.07.2022, 11:13

HANA AGENT

Security & Compliance



Overview by AoR / SAP Basis

SAP Basis

Baseline: STANDARD - SecurityBridge standard

Tag:

Search Reset

The AoR "SAP Basis" has 34 unique S&C Checks executed. A total of 576 use cases, across 5 systems, have been executed, resulting in 45 warnings and 259 errors

5001 - Security Audit Log Settings ⓘ 30 Checked 5 systems

5007 - SAP Component Check ⓘ 10 Checked 5 systems

5010 - HTTP Security Session Management ⓘ 5 Checked 5 systems

5012 - STAD Configuration Check ⓘ 15 Checked 5 systems

5013 - Limit Web-Enabled Content on ABAP ⓘ 30 Checked 5 systems

5015 - Message Server Security ⓘ 45 Checked 5 systems

5017 - Modification Protection ⓘ 5 Checked 5 systems

5018 - RFC Gateway Security ⓘ 50 Checked 5 systems

5023 - Read Access Logging ⚠ 5 Checked 5 systems

5024 - System settings to control SAP Logins ⓘ 60 Checked 5 systems

5025 - Transport Control Security ⓘ 40 Checked 5 systems

5028 - Profile parameters for update processes ⚠ 5 Checked 5 systems

5029 - Consistency of system parameters across application servers ☑ 5 Checked 5 systems

5030 - Broken update records ⓘ 15 Checked 5 systems

5032 - Old Lock Entries ☑ 10 Checked 5 systems

5034 - SAP Router ⓘ 9 Checked 5 systems

5035 - Obsolete clients ⓘ 5 Checked 5 systems

5037 - Web Dispatcher and ICM Security ⓘ 70 Checked 5 systems

5046 - Background Jobs ⓘ 30 Checked 5 systems

5048 - Secure Storage ☑ 5 Checked 5 systems

5050 - Kernel Vulnerabilities ⓘ 15 Checked 5 systems

5051 - Validate Security and housekeeping relevant jobs ⓘ 5 Checked 5 systems

5053 - Protection against Active Content ⓘ 5 Checked 5 systems

5055 - Missing Security Notes ⓘ 25 Checked 5 systems

5056 - Missing Oracle DB Patches ⓘ 7 Checked 2 systems

5061 - SAP Content Server ⓘ 15 Checked 5 systems

5070 - Standalone Web Dispatcher Validation ☑ 4 Checked 1 systems

7000 - HANA Auditing ☑ 10 Checked 2 systems

7001 - HANA Diagnosis Files ☑ 6 Checked 2 systems

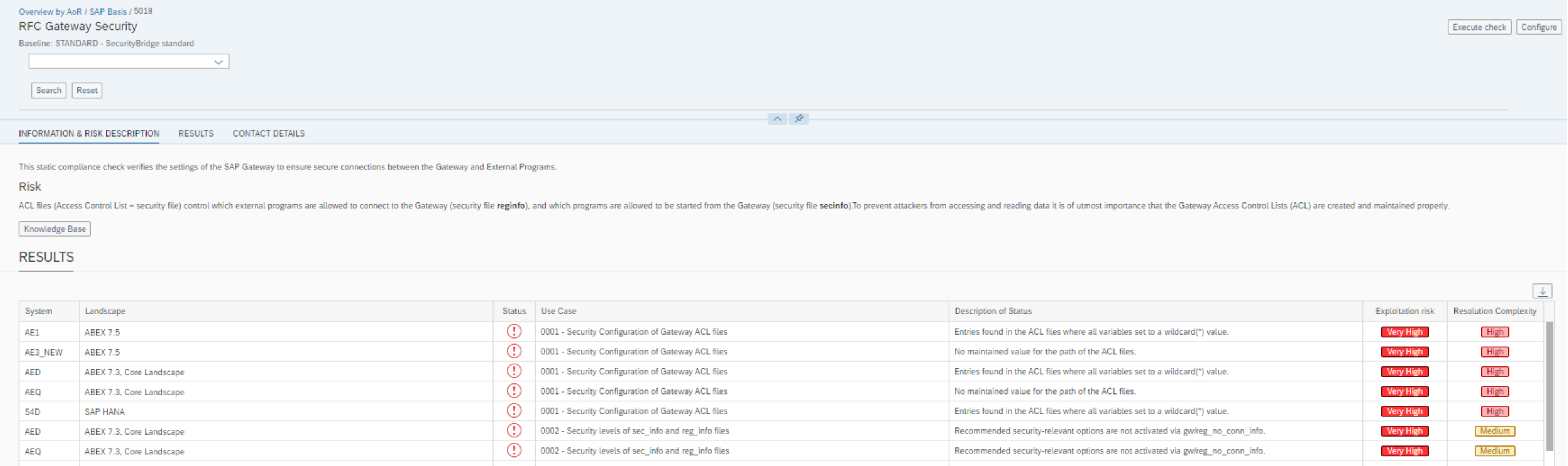
7003 - HANA Communications ⓘ 9 Checked 2 systems

7004 - HANA Tenant Databases ⚠ 4 Checked 2 systems

7007 - HANA Data Persistence ⚠ 4 Checked 2 systems

7008 - HANA Database Revision ☑ 2 Checked 2 systems

7009 - HANA Landscape Overview ⓘ 16 Checked 2 systems



Overview by AoR / SAP Basis / 5018

RFC Gateway Security

Baseline: STANDARD - SecurityBridge standard

Search Reset

Execute check Configure

INFORMATION & RISK DESCRIPTION RESULTS CONTACT DETAILS

This static compliance check verifies the settings of the SAP Gateway to ensure secure connections between the Gateway and External Programs.

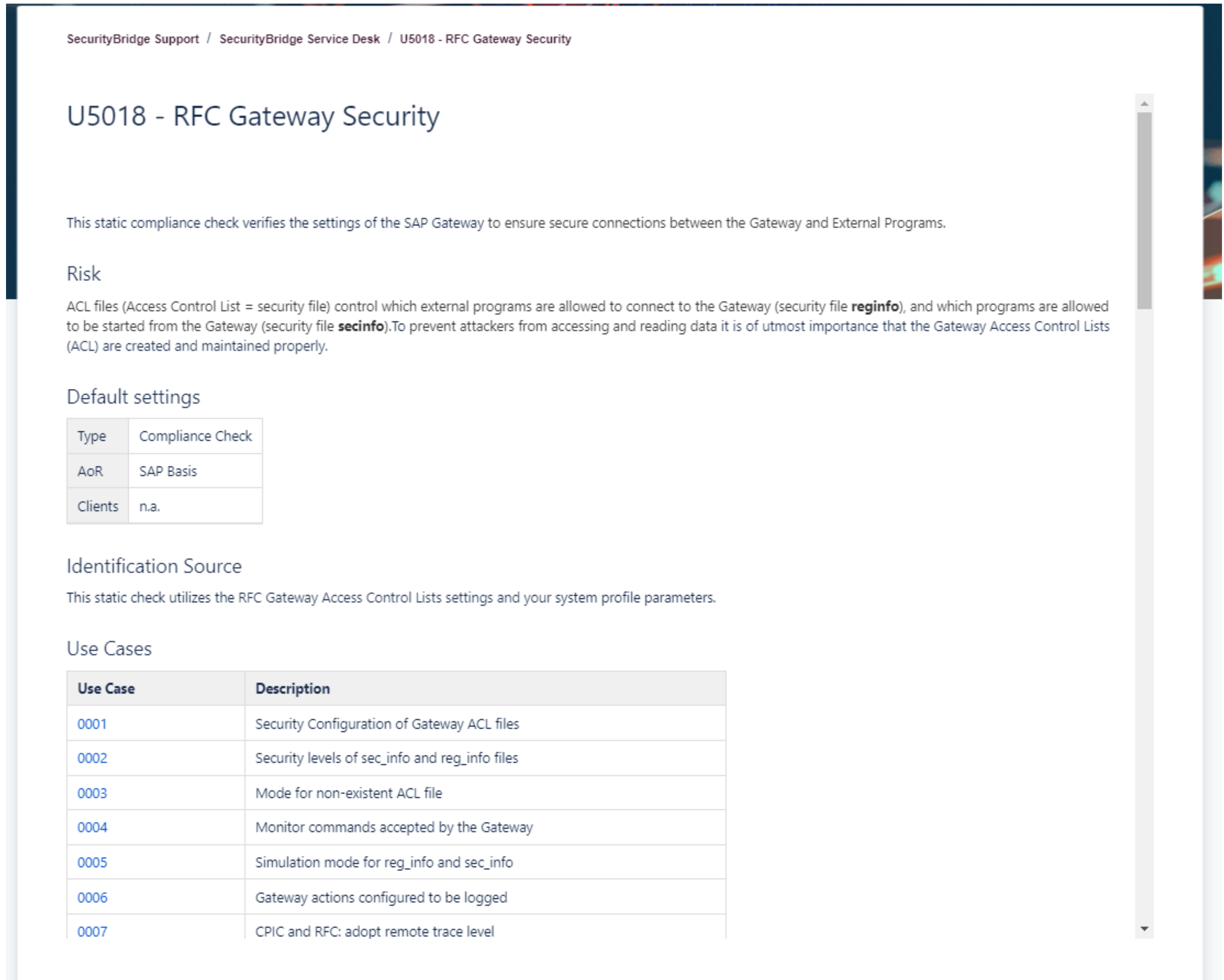
Risk

ACL files (Access Control List = security file) control which external programs are allowed to connect to the Gateway (security file **reginfo**), and which programs are allowed to be started from the Gateway (security file **secinfo**).To prevent attackers from accessing and reading data it is of utmost importance that the Gateway Access Control Lists (ACL) are created and maintained properly.

Knowledge Base

RESULTS

System	Landscape	Status	Use Case	Description of Status	Exploitation risk	Resolution Complexity
AE1	ABEX 7.5	ⓘ	0001 - Security Configuration of Gateway ACL files	Entries found in the ACL files where all variables set to a wildcard(*) value.	Very High	High
AE3_NEW	ABEX 7.5	ⓘ	0001 - Security Configuration of Gateway ACL files	No maintained value for the path of the ACL files.	Very High	High
AED	ABEX 7.3, Core Landscape	ⓘ	0001 - Security Configuration of Gateway ACL files	Entries found in the ACL files where all variables set to a wildcard(*) value.	Very High	High
AEQ	ABEX 7.3, Core Landscape	ⓘ	0001 - Security Configuration of Gateway ACL files	No maintained value for the path of the ACL files.	Very High	High
S4D	SAP HANA	ⓘ	0001 - Security Configuration of Gateway ACL files	Entries found in the ACL files where all variables set to a wildcard(*) value.	Very High	High
AED	ABEX 7.3, Core Landscape	ⓘ	0002 - Security levels of sec_info and reg_info files	Recommended security-relevant options are not activated via gw/reg_no_conn_info.	Very High	Medium
AEQ	ABEX 7.3, Core Landscape	ⓘ	0002 - Security levels of sec_info and reg_info files	Recommended security-relevant options are not activated via gw/reg_no_conn_info.	Very High	Medium



SecurityBridge Support / SecurityBridge Service Desk / U5018 - RFC Gateway Security

U5018 - RFC Gateway Security

This static compliance check verifies the settings of the SAP Gateway to ensure secure connections between the Gateway and External Programs.

Risk

ACL files (Access Control List = security file) control which external programs are allowed to connect to the Gateway (security file **reginfo**), and which programs are allowed to be started from the Gateway (security file **secinfo**).To prevent attackers from accessing and reading data it is of utmost importance that the Gateway Access Control Lists (ACL) are created and maintained properly.

Default settings

Type	Compliance Check
AoR	SAP Basis
Clients	n.a.

Identification Source

This static check utilizes the RFC Gateway Access Control Lists settings and your system profile parameters.

Use Cases

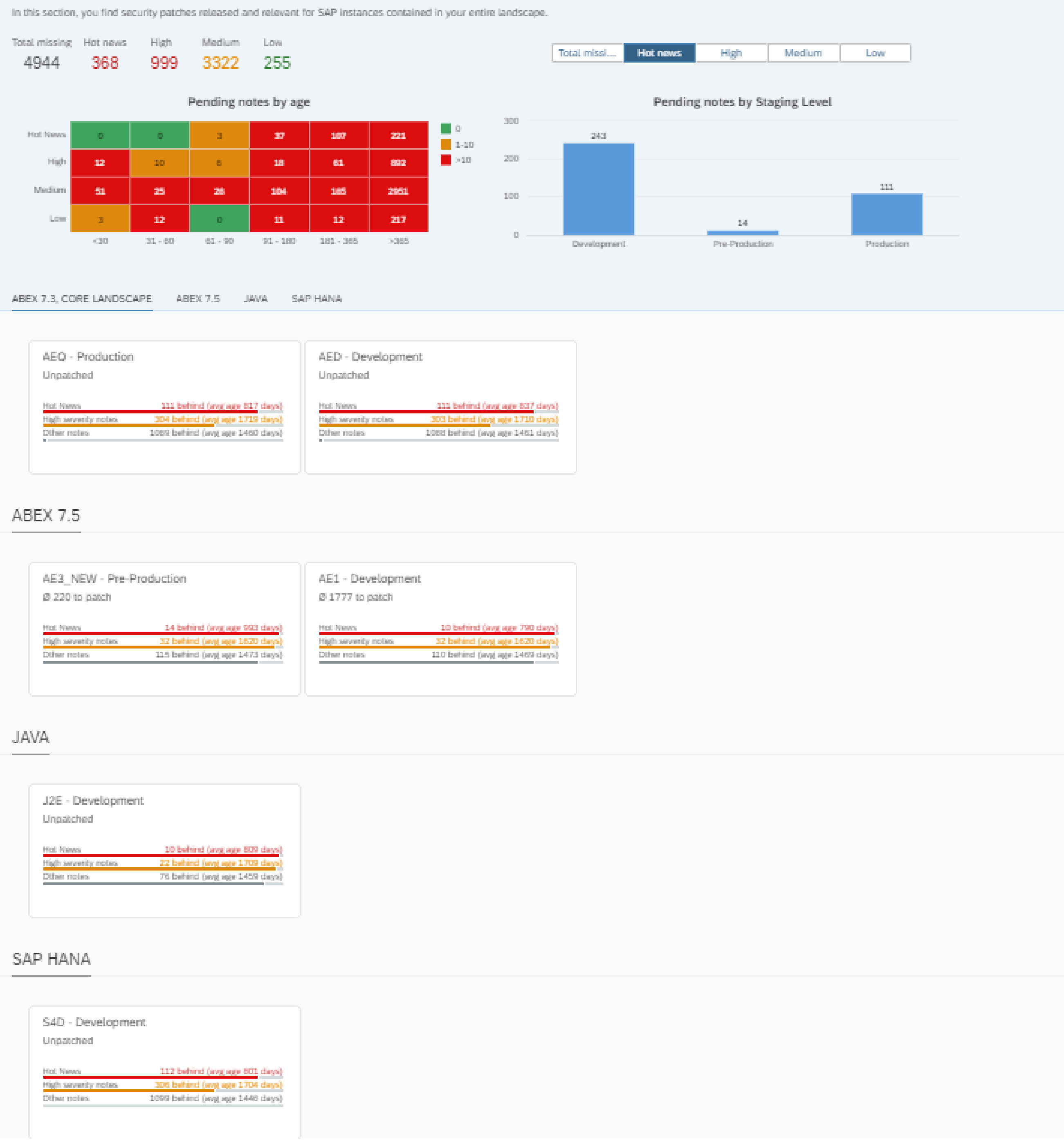
Use Case	Description
0001	Security Configuration of Gateway ACL files
0002	Security levels of sec_info and reg_info files
0003	Mode for non-existent ACL file
0004	Monitor commands accepted by the Gateway
0005	Simulation mode for reg_info and sec_info
0006	Gateway actions configured to be logged
0007	CPIC and RFC: adopt remote trace level

Security Bridge

Patch Management

Ensure that you system is up to date on SAP Security patches

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



In this section, you find security patches released and relevant for SAP instances contained in your entire landscape.

Total missing	Hot news	High	Medium	Low
4944	368	999	3322	255

Pending notes by age

	<30	31 - 60	61 - 90	91 - 180	181 - 365	>365
Hot News	0	0	3	37	107	221
High	12	10	6	18	61	892
Medium	51	25	26	104	185	2951
Low	3	12	0	11	12	217

Pending notes by Staging Level

AEQ - Production
Unpatched

Hot News	111 behind (avg age 817 days)
High severity notes	304 behind (avg age 1719 days)
Other notes	1089 behind (avg age 1460 days)

AED - Development
Unpatched

Hot News	111 behind (avg age 837 days)
High severity notes	303 behind (avg age 1710 days)
Other notes	1088 behind (avg age 1461 days)

ABEX 7.5

AE3_NEW - Pre-Production
Ø 220 to patch

Hot News	14 behind (avg age 993 days)
High severity notes	32 behind (avg age 1620 days)
Other notes	115 behind (avg age 1473 days)

AE1 - Development
Ø 1777 to patch

Hot News	10 behind (avg age 790 days)
High severity notes	32 behind (avg age 1620 days)
Other notes	110 behind (avg age 1469 days)

JAVA

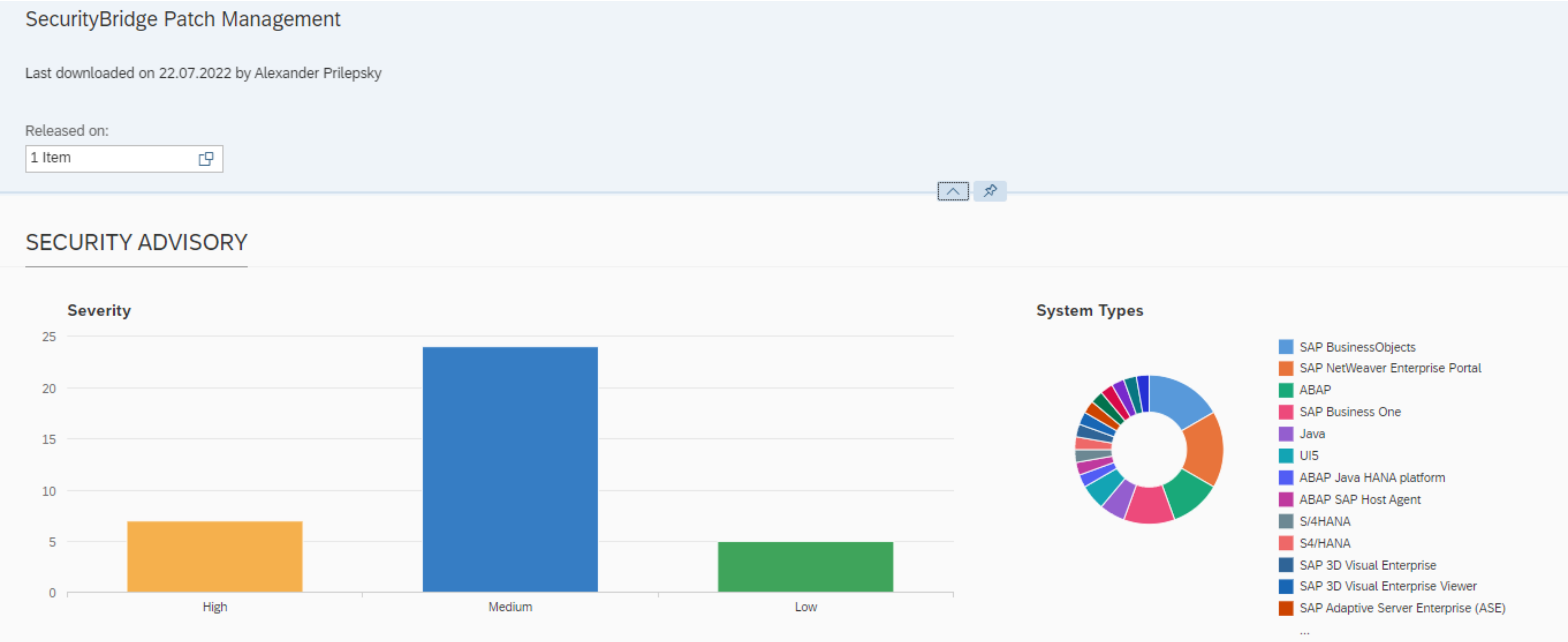
J2E - Development
Unpatched

Hot News	10 behind (avg age 809 days)
High severity notes	22 behind (avg age 1709 days)
Other notes	76 behind (avg age 1459 days)

SAP HANA

S4D - Development
Unpatched

Hot News	112 behind (avg age 801 days)
High severity notes	306 behind (avg age 1704 days)
Other notes	1099 behind (avg age 1446 days)



SecurityBridge Patch Management

Last downloaded on 22.07.2022 by Alexander Prilepsky

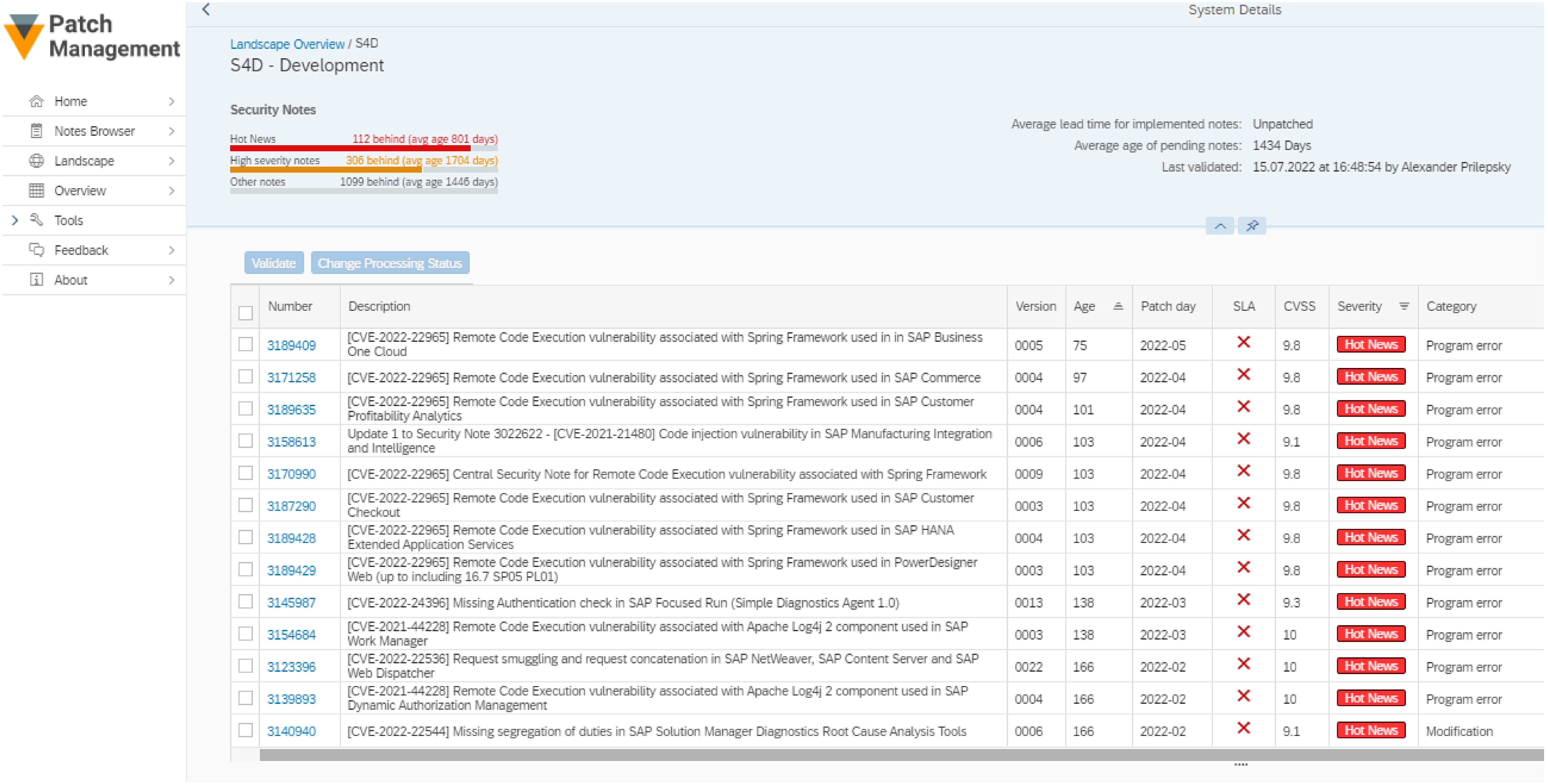
Released on:
1 Item

SECURITY ADVISORY

Severity

System Types

Patch Management



Landscape Overview / S4D

S4D - Development

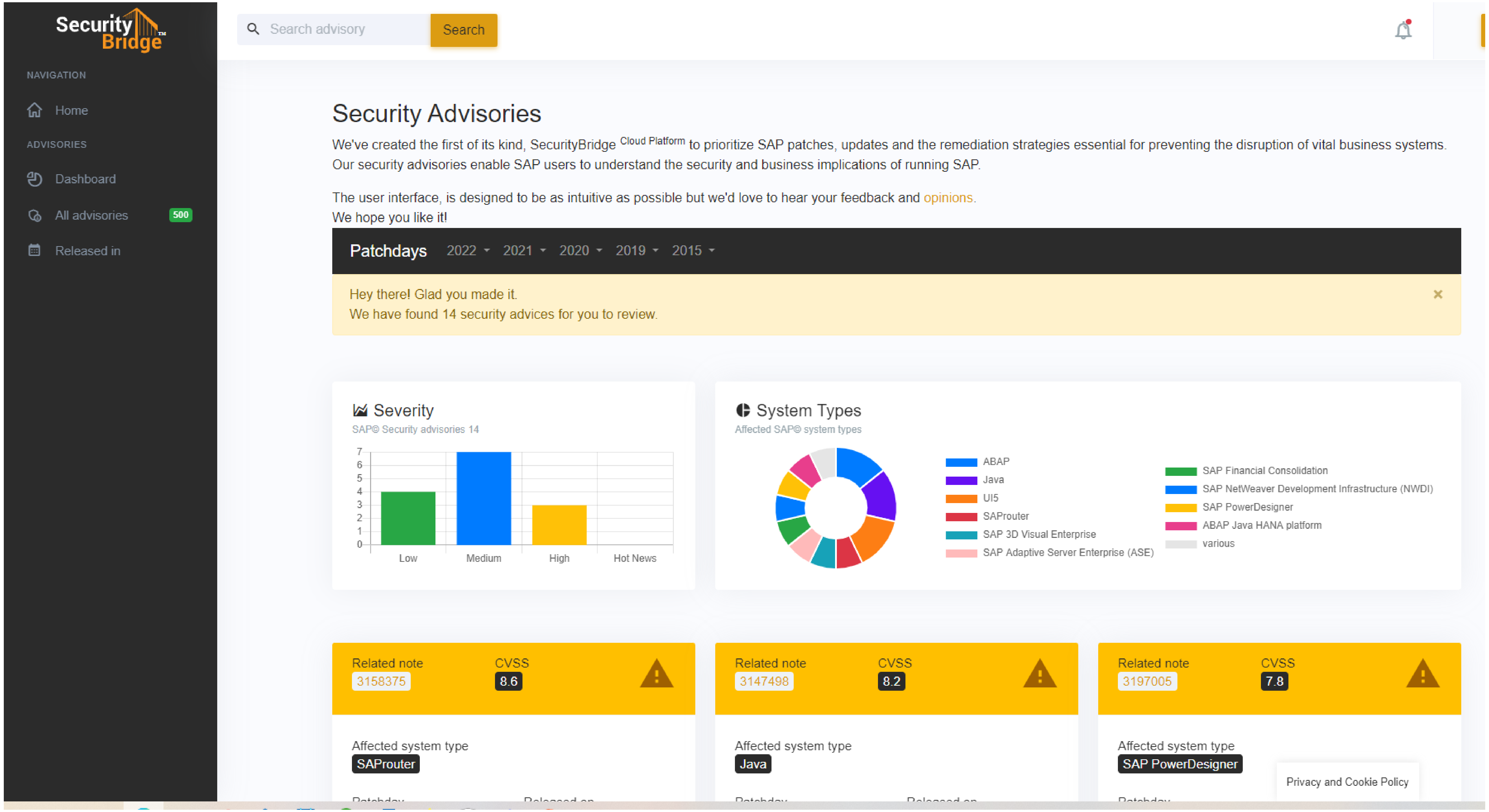
Security Notes

Hot News 112 behind (avg age 801 days)
High severity notes 306 behind (avg age 1704 days)
Other notes 1099 behind (avg age 1446 days)

Average lead time for implemented notes: Unpatched
Average age of pending notes: 1434 Days
Last validated: 15.07.2022 at 16:48:54 by Alexander Prilepsky

□	Number	Description	Version	Age	Patch day	SLA	CVSS	Severity	Category
□	3189409	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in in SAP Business One Cloud	0005	75	2022-05	✗	9.8	Hot News	Program error
□	3171258	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Commerce	0004	97	2022-04	✗	9.8	Hot News	Program error
□	3189635	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Customer Profitability Analytics	0004	101	2022-04	✗	9.8	Hot News	Program error
□	3158613	Update 1 to Security Note 3022622 - [CVE-2021-21480] Code injection vulnerability in SAP Manufacturing Integration and Intelligence	0006	103	2022-04	✗	9.1	Hot News	Program error
□	3170990	[CVE-2022-22965] Central Security Note for Remote Code Execution vulnerability associated with Spring Framework	0009	103	2022-04	✗	9.8	Hot News	Program error
□	3187290	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP Customer Checkout	0003	103	2022-04	✗	9.8	Hot News	Program error
□	3189428	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in SAP HANA Extended Application Services	0004	103	2022-04	✗	9.8	Hot News	Program error
□	3189429	[CVE-2022-22965] Remote Code Execution vulnerability associated with Spring Framework used in PowerDesigner Web (up to including 16.7 SP05 PL01)	0003	103	2022-04	✗	9.8	Hot News	Program error
□	3145987	[CVE-2022-24396] Missing Authentication check in SAP Focused Run (Simple Diagnostics Agent 1.0)	0013	138	2022-03	✗	9.3	Hot News	Program error
□	3154684	[CVE-2021-44228] Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Work Manager	0003	138	2022-03	✗	10	Hot News	Program error
□	3123396	[CVE-2022-22536] Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher	0022	166	2022-02	✗	10	Hot News	Program error
□	3139893	[CVE-2021-44228] Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Dynamic Authorization Management	0004	166	2022-02	✗	10	Hot News	Program error
□	3140940	[CVE-2022-22544] Missing segregation of duties in SAP Solution Manager Diagnostics Root Cause Analysis Tools	0006	166	2022-02	✗	9.1	Hot News	Modification

Patch Management



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!

Hey there! Glad you made it.
We have found 14 security advices for you to review.

Severity

SAP® Security advisories 14

System Types

Affected SAP® system types

ABAP
Java
UI5
SAProuter
SAP 3D Visual Enterprise
SAP Adaptive Server Enterprise (ASE)
SAP Financial Consolidation
SAP NetWeaver Development Infrastructure (NWDI)
SAP PowerDesigner
ABAP Java HANA platform
various

Related note	CVSS
3158375	8.6

Affected system type
SAProuter

Patchday Released on

Related note	CVSS
3147498	8.2

Affected system type
Java

Patchday Released on

Related note	CVSS
3197005	7.8

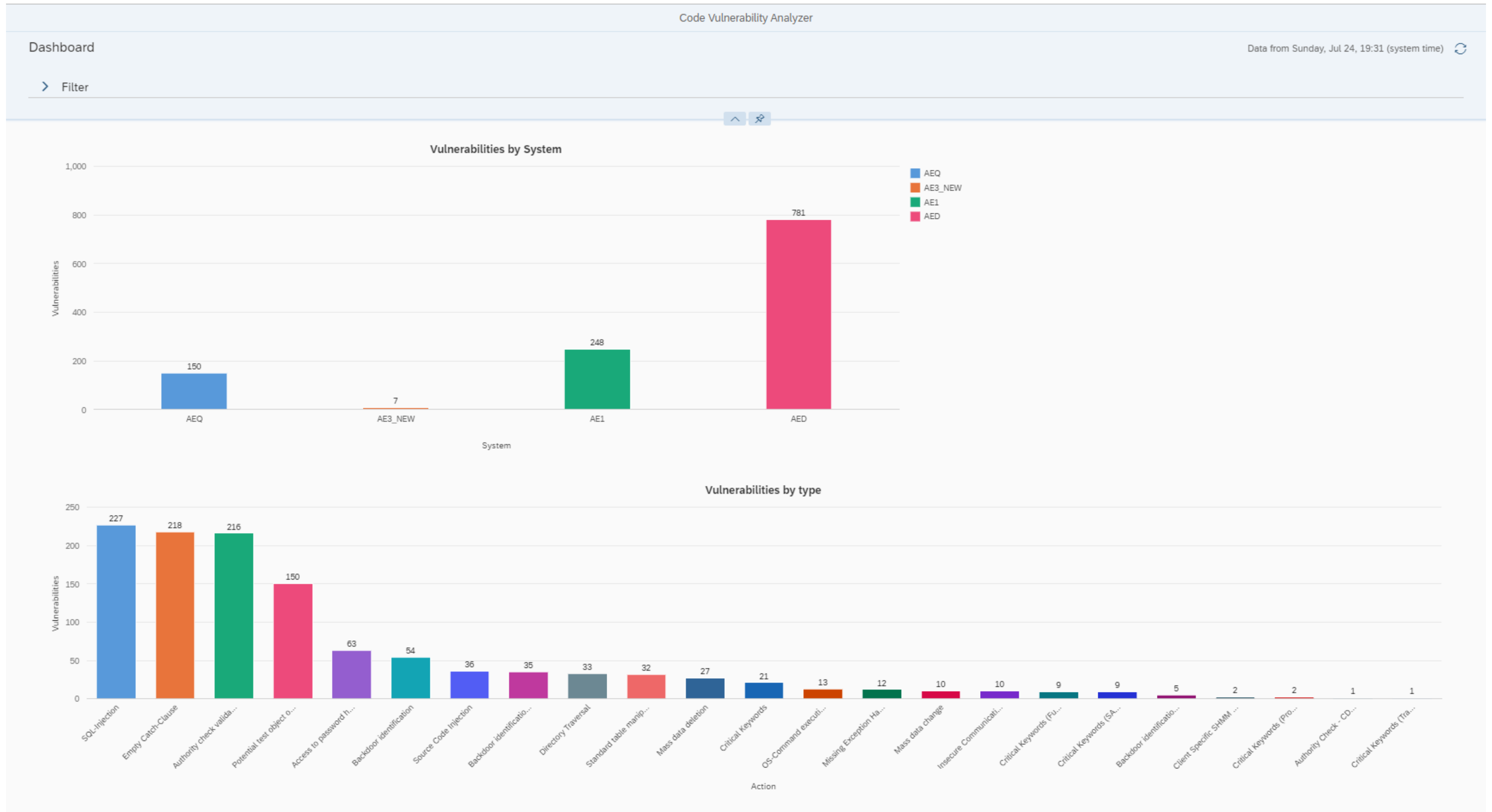
Affected system type
SAP PowerDesigner

Patchday

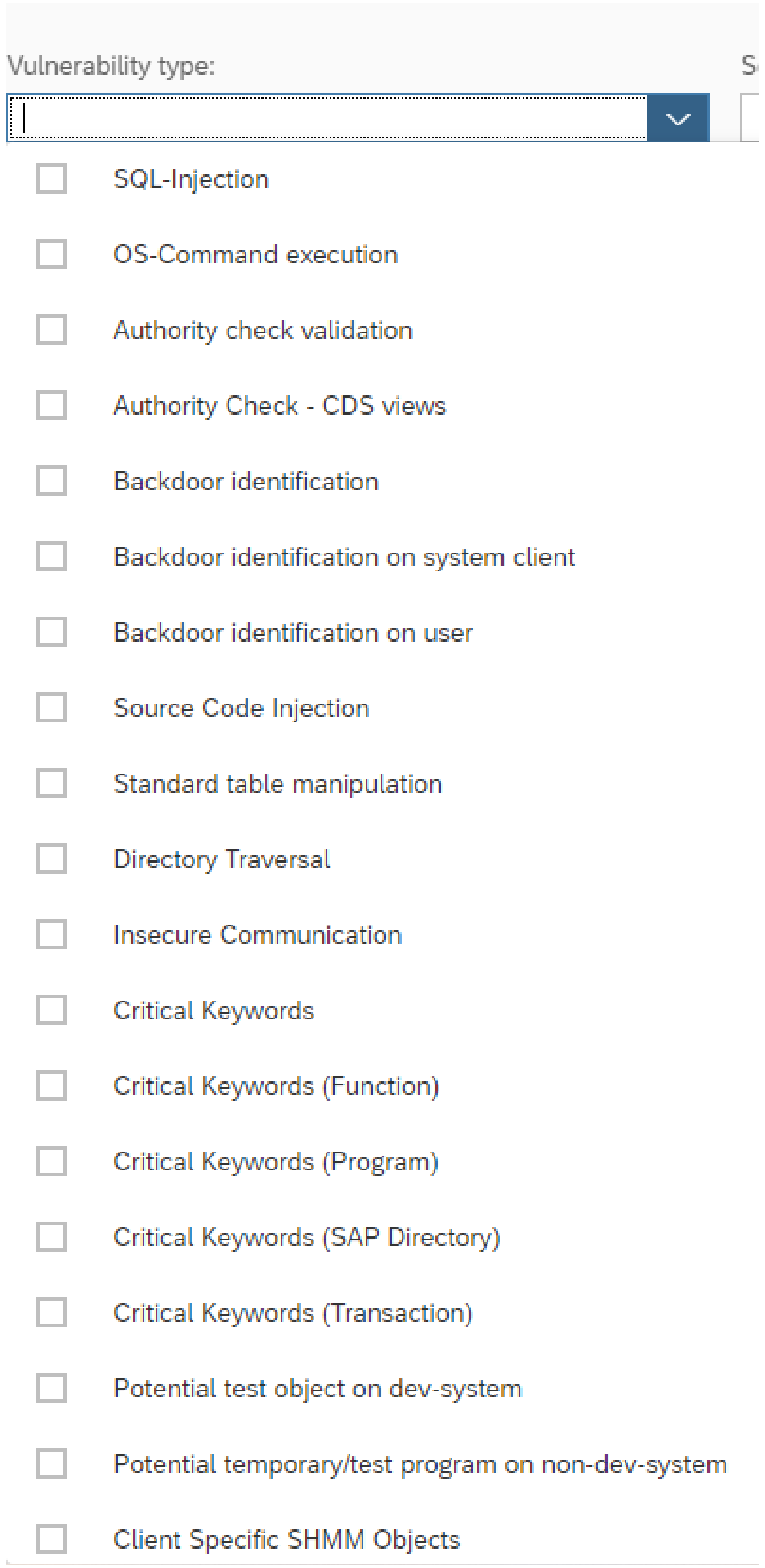
Privacy and Cookie Policy

Code Vulnerability Analysis

Scanning custom code to ensure security risks are identified and addressed



Data from Sunday, Jul 24, 19:31 (system time)



Vulnerability type:

S

☐ 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)

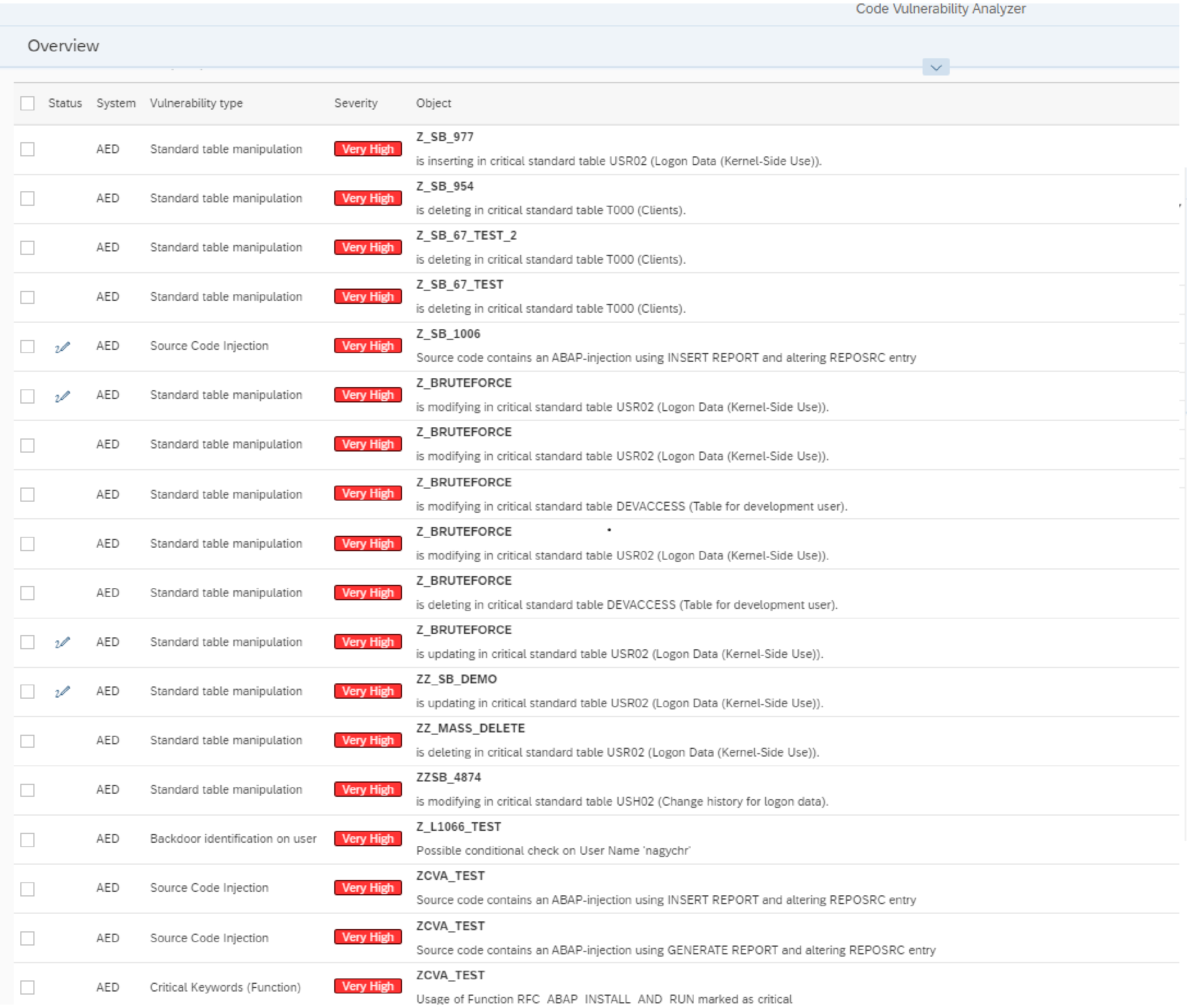
☐ Potential test object on dev-system

☐ Potential temporary/test program on non-dev-system

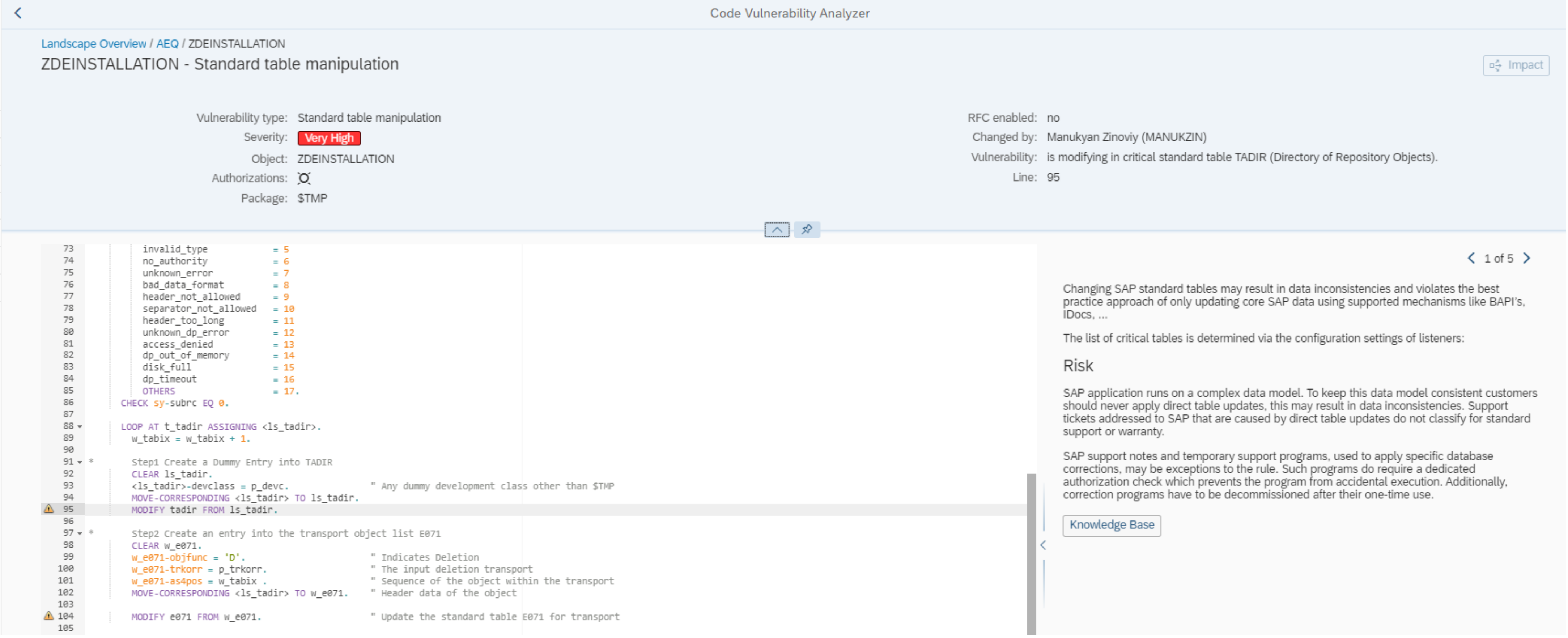
☐ Client Specific SHMM Objects

SecurityBridge

Code Vulnerability Analyzer



□	Status	System	Vulnerability type	Severity	Object
□		AED	Standard table manipulation	Very High	Z_SB_977 is inserting in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□		AED	Standard table manipulation	Very High	Z_SB_954 is deleting in critical standard table T000 (Clients).
□		AED	Standard table manipulation	Very High	Z_SB_67_TEST_2 is deleting in critical standard table T000 (Clients).
□		AED	Standard table manipulation	Very High	Z_SB_67_TEST is deleting in critical standard table T000 (Clients).
□	✎	AED	Source Code Injection	Very High	Z_SB_1006 Source code contains an ABAP-injection using INSERT REPORT and altering REPOSRC entry
□	✎	AED	Standard table manipulation	Very High	Z_BRUTEFORCE is modifying in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□		AED	Standard table manipulation	Very High	Z_BRUTEFORCE is modifying in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□		AED	Standard table manipulation	Very High	Z_BRUTEFORCE is modifying in critical standard table DEVACCESS (Table for development user).
□		AED	Standard table manipulation	Very High	Z_BRUTEFORCE is modifying in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□		AED	Standard table manipulation	Very High	Z_BRUTEFORCE is deleting in critical standard table DEVACCESS (Table for development user).
□	✎	AED	Standard table manipulation	Very High	Z_BRUTEFORCE is updating in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□	✎	AED	Standard table manipulation	Very High	ZZ_SB_DEMO is updating in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□		AED	Standard table manipulation	Very High	ZZ_MASS_DELETE is deleting in critical standard table USR02 (Logon Data (Kernel-Side Use)).
□		AED	Standard table manipulation	Very High	ZZSB_4874 is modifying in critical standard table USH02 (Change history for logon data).
□		AED	Backdoor identification on user	Very High	Z_L1066_TEST Possible conditional check on User Name 'nagychr'
□		AED	Source Code Injection	Very High	ZCVA_TEST Source code contains an ABAP-injection using INSERT REPORT and altering REPOSRC entry
□		AED	Source Code Injection	Very High	ZCVA_TEST Source code contains an ABAP-injection using GENERATE REPORT and altering REPOSRC entry
□		AED	Critical Keywords (Function)	Very High	ZCVA_TEST Usage of Function RFC ABAP INSTALL AND RUN marked as critical



Code Vulnerability Analyzer
Landscape Overview / AEQ / ZDEINSTALLATION
Impact

ZDEINSTALLATION - Standard table manipulation

Vulnerability type: Standard table manipulation
Severity: Very High
Object: ZDEINSTALLATION
Authorizations: ⭘
Package: $TMP

RFC enabled: no
Changed by: Manukyan Zinoviy (MANUKZIN)
Vulnerability: is modifying in critical standard table TADIR (Directory of Repository Objects).
Line: 95

```
 73          invalid_type          = 5
 74          no_authority          = 6
 75          unknown_error         = 7
 76          bad_data_format       = 8
 77          header_not_allowed    = 9
 78          separator_not_allowed = 10
 79          header_too_long       = 11
 80          unknown_dp_error      = 12
 81          access_denied         = 13
 82          dp_out_of_memory      = 14
 83          disk_full             = 15
 84          dp_timeout            = 16
 85          OTHERS                = 17.
 86      CHECK sy-subrc EQ 0.
 87
 88      LOOP AT t_tadir ASSIGNING <ls_tadir>.
 89        w_tabix = w_tabix + 1.
 90
 91 *      Step1 Create a Dummy Entry into TADIR
 92        CLEAR ls_tadir.
 93        <ls_tadir>-devclass = p_devc.               " Any dummy development class other than $TMP
 94        MOVE-CORRESPONDING <ls_tadir> TO ls_tadir.
 95        MODIFY tadir FROM ls_tadir.
 96
 97 *      Step2 Create an entry into the transport object list E071
 98        CLEAR w_e071.
 99        w_e071-objfunc = 'D'.                       " Indicates Deletion
100        w_e071-trkorr = p_trkorr.                   " The input deletion transport
101        w_e071-as4pos = w_tabix .                   " Sequence of the object within the transport
102        MOVE-CORRESPONDING <ls_tadir> TO w_e071.    " Header data of the object
103
104        MODIFY e071 FROM w_e071.                    " Update the standard table E071 for transport
105
```

Changing SAP standard tables may result in data inconsistencies and violates the best practice approach of only updating core SAP data using supported mechanisms like BAPI's, IDocs, ...

The list of critical tables is determined via the configuration settings of listeners:

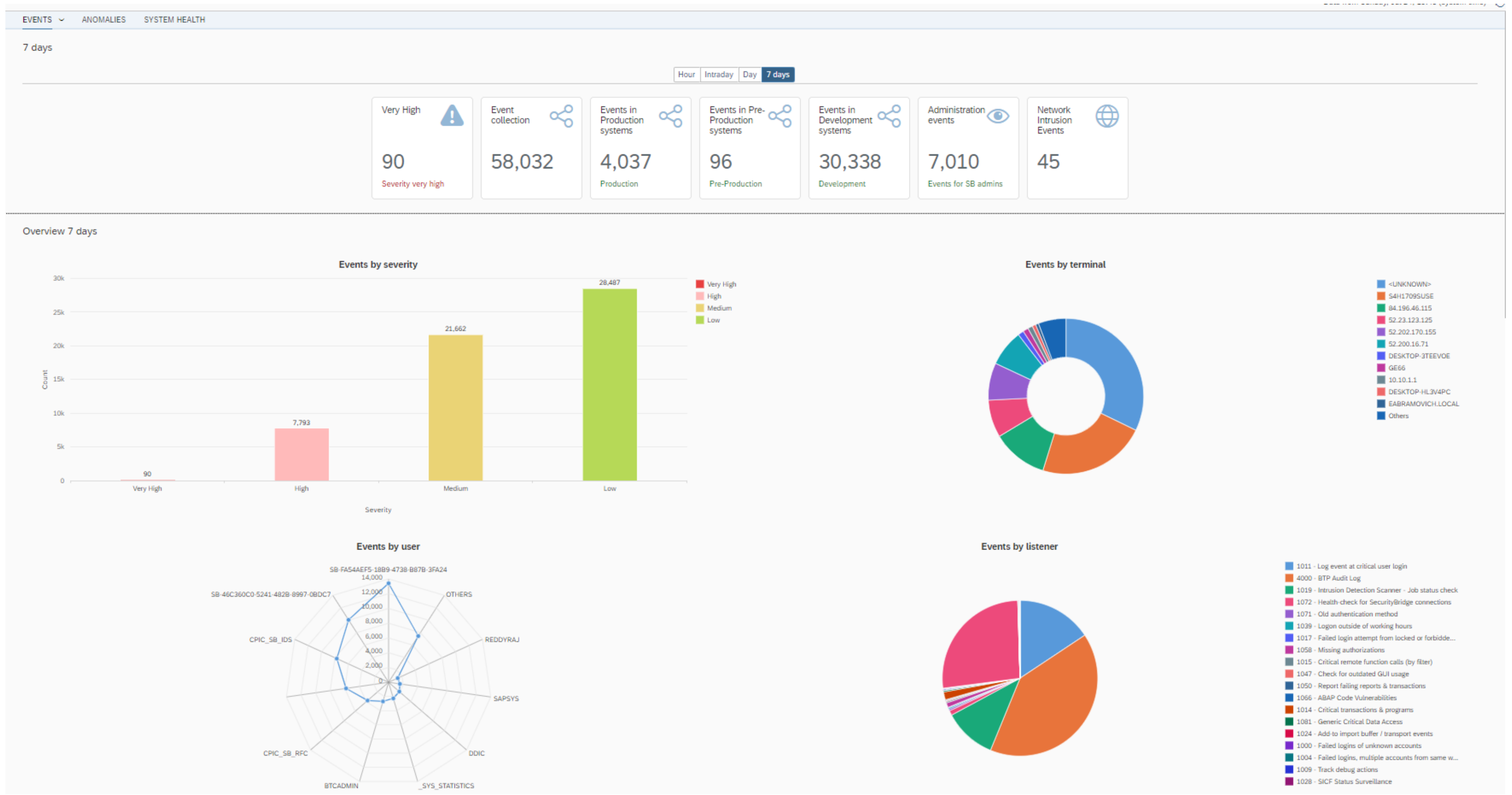
Risk

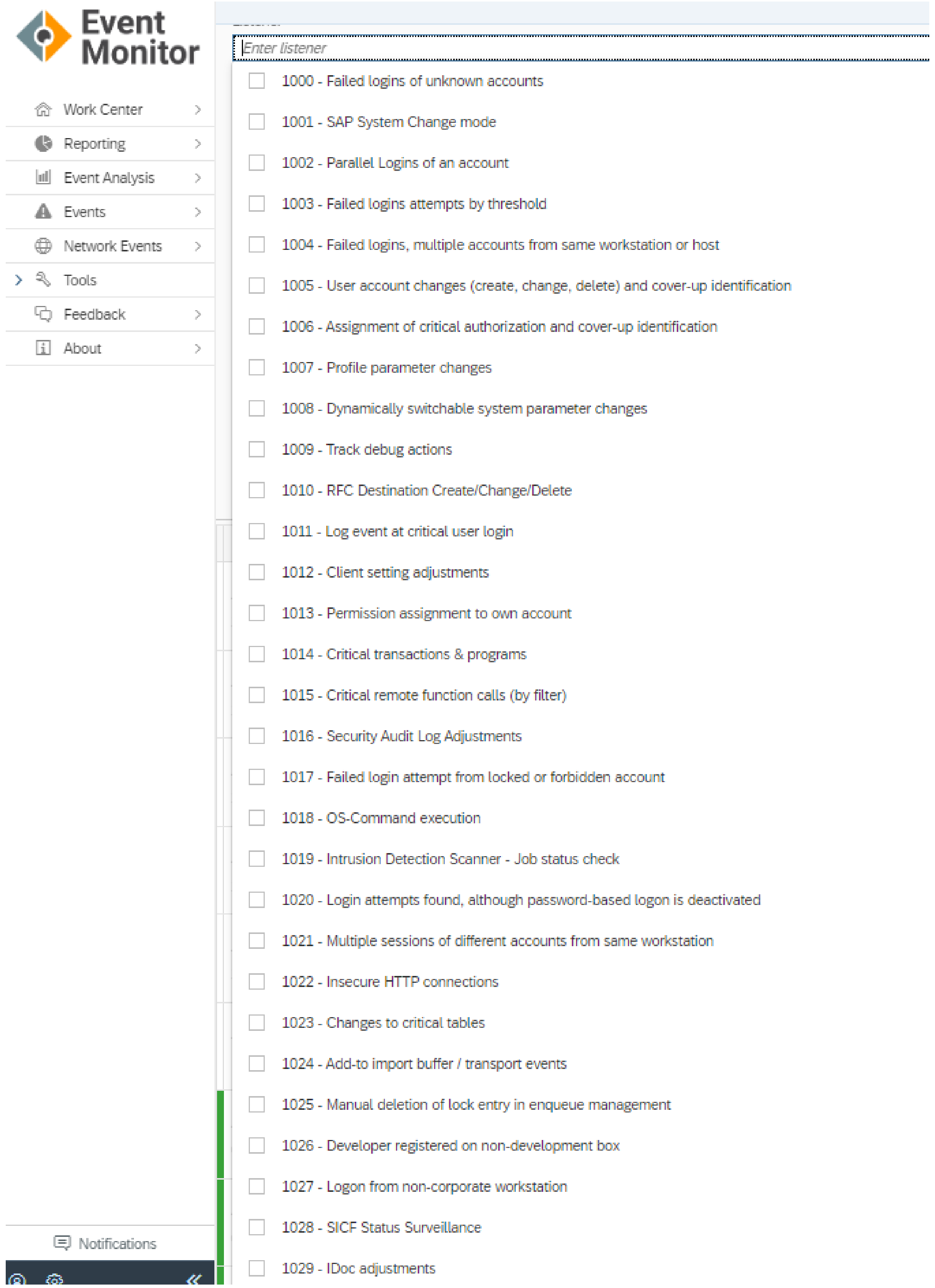
SAP application runs on a complex data model. To keep this data model consistent customers should never apply direct table updates, this may result in data inconsistencies. Support tickets addressed to SAP that are caused by direct table updates do not classify for standard support or warranty.

SAP support notes and temporary support programs, used to apply specific database corrections, may be exceptions to the rule. Such programs do require a dedicated authorization check which prevents the program from accidental execution. Additionally, correction programs have to be decommissioned after their one-time use.

Event Monitoring (Intrusion Detection System) - IDS

Continuously scanning all logs and audit sources within the SAP instance for SAP-specific attack patterns and zero-day vulnerabilities.

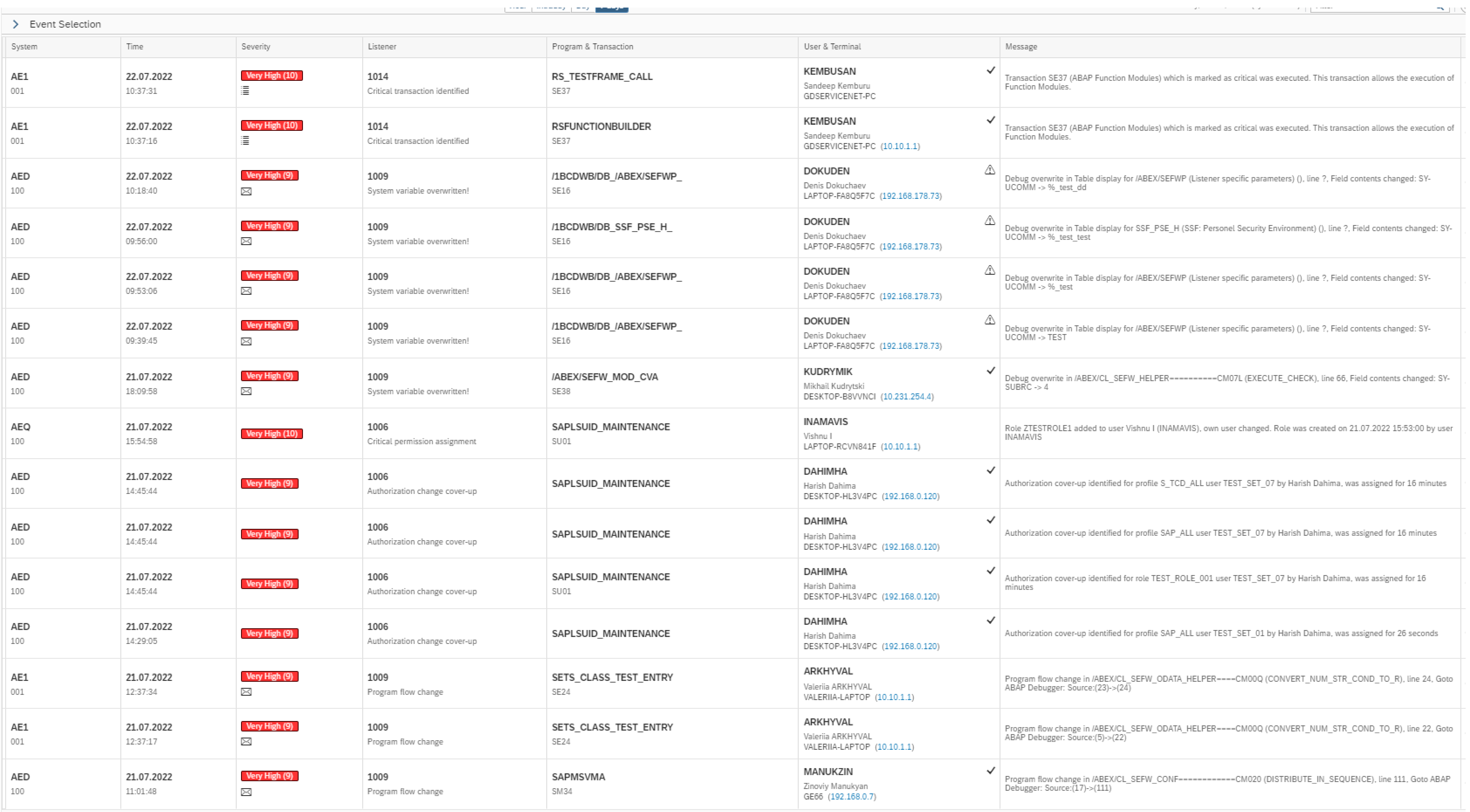




Enter listener

- □ 1000 - Failed logins of unknown accounts
- □ 1001 - SAP System Change mode
- □ 1002 - Parallel Logins of an account
- □ 1003 - Failed logins attempts by threshold
- □ 1004 - Failed logins, multiple accounts from same workstation or host
- □ 1005 - User account changes (create, change, delete) and cover-up identification
- □ 1006 - Assignment of critical authorization and cover-up identification
- □ 1007 - Profile parameter changes
- □ 1008 - Dynamically switchable system parameter changes
- □ 1009 - Track debug actions
- □ 1010 - RFC Destination Create/Change/Delete
- □ 1011 - Log event at critical user login
- □ 1012 - Client setting adjustments
- □ 1013 - Permission assignment to own account
- □ 1014 - Critical transactions & programs
- □ 1015 - Critical remote function calls (by filter)
- □ 1016 - Security Audit Log Adjustments
- □ 1017 - Failed login attempt from locked or forbidden account
- □ 1018 - OS-Command execution
- □ 1019 - Intrusion Detection Scanner - Job status check
- □ 1020 - Login attempts found, although password-based logon is deactivated
- □ 1021 - Multiple sessions of different accounts from same workstation
- □ 1022 - Insecure HTTP connections
- □ 1023 - Changes to critical tables
- □ 1024 - Add-to import buffer / transport events
- □ 1025 - Manual deletion of lock entry in enqueue management
- □ 1026 - Developer registered on non-development box
- □ 1027 - Logon from non-corporate workstation
- □ 1028 - SICF Status Surveillance
- □ 1029 - IDoc adjustments

Event Monitor



Event Selection

System	Time	Severity	Listener	Program & Transaction	User & Terminal	Message
AE1 001	22.07.2022 10:37:31	Very High (10) ☰	1014 Critical transaction identified	RS_TESTFRAME_CALL SE37	KEMBUSAN ✓ Sandeep Kemburu GDSERVICENET-PC	Transaction SE37 (ABAP Function Modules) which is marked as critical was executed. This transaction allows the execution of Function Modules.
AE1 001	22.07.2022 10:37:16	Very High (10) ☰	1014 Critical transaction identified	RSFUNCTIONBUILDER SE37	KEMBUSAN ✓ Sandeep Kemburu GDSERVICENET-PC (10.10.1.1)	Transaction SE37 (ABAP Function Modules) which is marked as critical was executed. This transaction allows the execution of Function Modules.
AED 100	22.07.2022 10:18:40	Very High (9) ✉	1009 System variable overwritten!	/1BCDWB/DB_/ABEX/SEFWP_ SE16	DOKUDEN ⚠ Denis Dokuchaev LAPTOP-FA8Q5F7C (192.168.178.73)	Debug overwrite in Table display for /ABEX/SEFWP (Listener specific parameters) (), line ?, Field contents changed: SY-UCOMM -> %_test_dd
AED 100	22.07.2022 09:56:00	Very High (9) ✉	1009 System variable overwritten!	/1BCDWB/DB_SSF_PSE_H_ SE16	DOKUDEN ⚠ Denis Dokuchaev LAPTOP-FA8Q5F7C (192.168.178.73)	Debug overwrite in Table display for SSF_PSE_H (SSF: Personel Security Environment) (), line ?, Field contents changed: SY-UCOMM -> %_test_test
AED 100	22.07.2022 09:53:06	Very High (9) ✉	1009 System variable overwritten!	/1BCDWB/DB_/ABEX/SEFWP_ SE16	DOKUDEN ⚠ Denis Dokuchaev LAPTOP-FA8Q5F7C (192.168.178.73)	Debug overwrite in Table display for /ABEX/SEFWP (Listener specific parameters) (), line ?, Field contents changed: SY-UCOMM -> %_test
AED 100	22.07.2022 09:39:45	Very High (9) ✉	1009 System variable overwritten!	/1BCDWB/DB_/ABEX/SEFWP_ SE16	DOKUDEN ⚠ Denis Dokuchaev LAPTOP-FA8Q5F7C (192.168.178.73)	Debug overwrite in Table display for /ABEX/SEFWP (Listener specific parameters) (), line ?, Field contents changed: SY-UCOMM -> TEST
AED 100	21.07.2022 18:09:58	Very High (9) ✉	1009 System variable overwritten!	/ABEX/SEFW_MOD_CVA SE38	KUDRYMIK ✓ Mikhail Kudrytski DESKTOP-B8VVNCI (10.231.254.4)	Debug overwrite in /ABEX/CL_SEFW_HELPER==========CM07L (EXECUTE_CHECK), line 66, Field contents changed: SY-SUBRC -> 4
AEQ 100	21.07.2022 15:54:58	Very High (10)	1006 Critical permission assignment	SAPLSUID_MAINTENANCE SU01	INAMAVIS Vishnu I LAPTOP-RCVN841F (10.10.1.1)	Role ZTESTROLE1 added to user Vishnu I (INAMAVIS), own user changed. Role was created on 21.07.2022 15:53:00 by user INAMAVIS
AED 100	21.07.2022 14:45:44	Very High (9)	1006 Authorization change cover-up	SAPLSUID_MAINTENANCE	DAHIMHA ✓ Harish Dahima DESKTOP-HL3V4PC (192.168.0.120)	Authorization cover-up identified for profile S_TCD_ALL user TEST_SET_07 by Harish Dahima, was assigned for 16 minutes
AED 100	21.07.2022 14:45:44	Very High (9)	1006 Authorization change cover-up	SAPLSUID_MAINTENANCE	DAHIMHA ✓ Harish Dahima DESKTOP-HL3V4PC (192.168.0.120)	Authorization cover-up identified for profile SAP_ALL user TEST_SET_07 by Harish Dahima, was assigned for 16 minutes
AED 100	21.07.2022 14:45:44	Very High (9)	1006 Authorization change cover-up	SAPLSUID_MAINTENANCE SU01	DAHIMHA ✓ Harish Dahima DESKTOP-HL3V4PC (192.168.0.120)	Authorization cover-up identified for role TEST_ROLE_001 user TEST_SET_07 by Harish Dahima, was assigned for 16 minutes
AED 100	21.07.2022 14:29:05	Very High (9)	1006 Authorization change cover-up	SAPLSUID_MAINTENANCE	DAHIMHA ✓ Harish Dahima DESKTOP-HL3V4PC (192.168.0.120)	Authorization cover-up identified for profile SAP_ALL user TEST_SET_01 by Harish Dahima, was assigned for 26 seconds
AE1 001	21.07.2022 12:37:34	Very High (9) ✉	1009 Program flow change	SETS_CLASS_TEST_ENTRY SE24	ARKHYVAL Valeriia ARKHYVAL VALERIIA-LAPTOP (10.10.1.1)	Program flow change in /ABEX/CL_SEFW_ODATA_HELPER====CM00Q (CONVERT_NUM_STR_COND_TO_R), line 24, Goto ABAP Debugger: Source:(23)->(24)
AE1 001	21.07.2022 12:37:17	Very High (9) ✉	1009 Program flow change	SETS_CLASS_TEST_ENTRY SE24	ARKHYVAL Valeriia ARKHYVAL VALERIIA-LAPTOP (10.10.1.1)	Program flow change in /ABEX/CL_SEFW_ODATA_HELPER====CM00Q (CONVERT_NUM_STR_COND_TO_R), line 22, Goto ABAP Debugger: Source:(5)->(22)
AED 100	21.07.2022 11:01:48	Very High (9) ✉	1009 Program flow change	SAPMSVMA SM34	MANUKZIN ✓ Zinoviy Manukyan GE66 (192.168.0.7)	Program flow change in /ABEX/CL_SEFW_CONF============CM020 (DISTRIBUTE_IN_SEQUENCE), line 111, Goto ABAP Debugger: Source:(17)->(111)

Summary

- You are the target, bad people want in!
- Hackers are getting in, and the IoT is just going to make that easier
- 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
- Monitoring what's going on (you will learn more about your SAP system then you ever imagined)
- You need to know where you stand – the first step is always the hardest

thank you.

SecurityBridge