



Pathlock Cybersecurity Application Controls for SAP

SAP Vulnerability Scanning and Remediation
Real Time Threat Detection
Code and Transport Scanning





Pathlock Cyber Application Control (CAC)



Complete protection for SAP Instances

Vulnerability and Patch Management

- 4000+ automated checks and security notes
- Scans all System layers and cross system
- Zero pen - testing expertise or SAP Cybersecurity expertise required
- 15 years of maturity in the product

Code Scanning

- 130+ Patterns enhancing the SAP Standard code checks
- Automatic execution of checks
- integrating into existing development process
- Seamless Integration into CVA, SCI and ATC

Transport Scanning

- 100+ testcases and checks
- Scanning content before export and import
- Scanning code, dev. objects and content

Threat detection and response

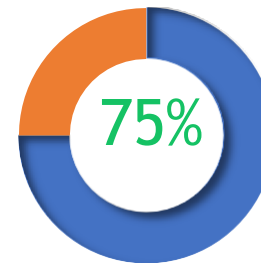
- 1500+ Threat signatures monitoring your SAP application 24/7/365
- Aggregating single noncritical events if contextual critical
- Data Loss Prevention
- Event forwarding OOTB to any SIEM

Executive Web Dashboard clearly showing your entire SAP Security Posture

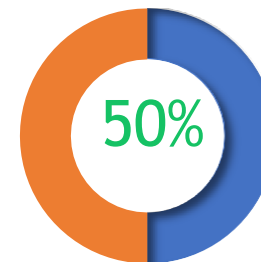
Defend | Threat detection & response

THREAT DETECTION

- **Continuous monitoring** and real-time alerts for over 4,000+ threat indicators
- **Prioritize alerts** based on stakeholder risk posture and/or systems
- **Respond quickly** to active threats via detailed alarm notifications
- **Analyze Root Cause** by sending threat information to SIEMs and correlating with other system logs



Improved incident response times



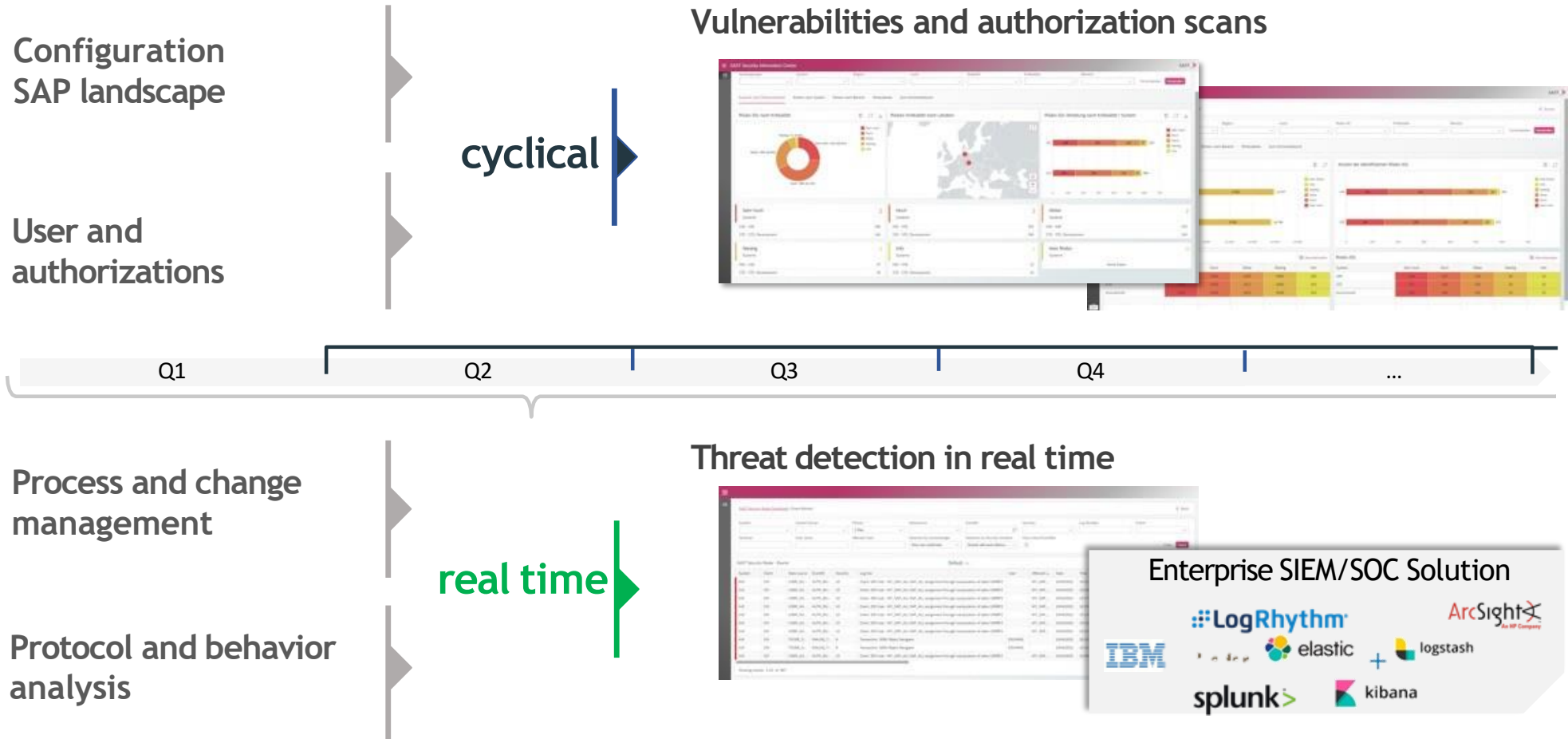
Reduced forensic investigation time



SAP log forwarding enables correlation with other logs

Protecting your Crown Jewels

Holistic SAP security view required – Cyclic checks in combination with real-time threat detection



Real Time Threat Detection Capabilities



Security Intelligence / SIEM / SOAR



Real time threat and attack detection for SAP systems.



Monitor critical transactions, applications, log files.



User behavior analytics in real time.



Cutting-edge ruleset for threat detection.



Super fast detection and alerting on suspicious log entries.



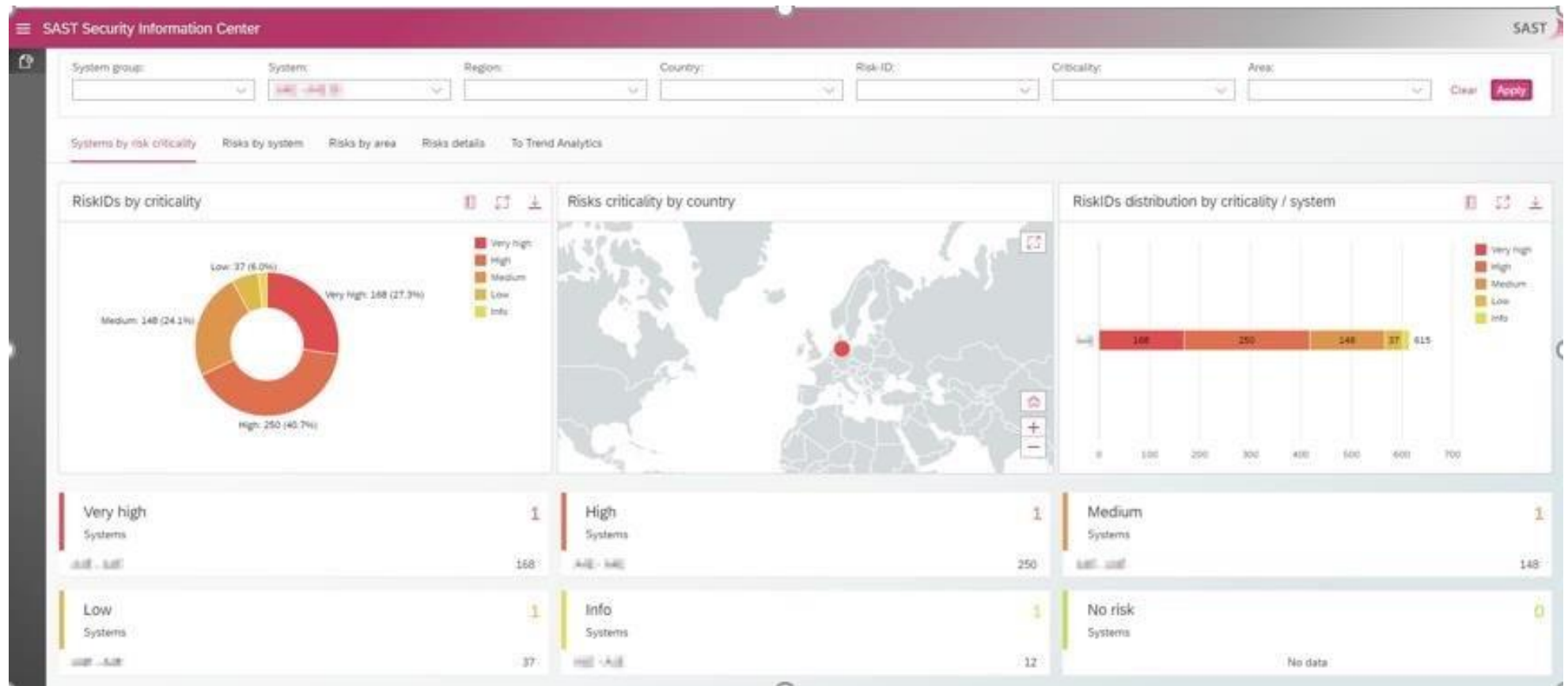
Export SAP threat / vulnerability information to enterprise SIEM solutions.



Establish global SAP security dashboards.

Unified, Cloud Cybersecurity Cockpit

Monitor and resolve threats across the enterprise as they evolve, staying one step ahead



Holistic SAP security view with Pathlock

How to implement baseline compliance checks and threat detection for SAP systems

Solution Brief

System Security Validation protects on-premise, cloud and hybrid SAP systems including Netweaver, S/4HANA, ABAP and J2EE platforms.

The solution provides real-time analyses for security baseline compliance control and vulnerability detection.

The predefined master policy contains 3300+ test cases and can easily be adopted to any customer or policy requirements.

Security Radar delivers cutting-edge and real-time threat detection capabilities combined with SIEM integration to all major SIEM products. The ruleset contains 1200+ threat and attack detection patterns.

Key Features

- ▶ Simple and fast Deployment
- ▶ No additional hardware required
- ▶ Realtime Vulnerability and Anomaly Detection
- ▶ Predefined Security Baseline Policies
- ▶ Compliance Reporting and Integrated Dashboards
- ▶ Scanning for missing security notes
- ▶ Interface Monitoring
- ▶ Code Security Scanning
- ▶ Realtime Threat and Attack Detection
- ▶ SIEM Integration

Typical use cases where Pathlock CAC supports security analysts:



Platform Security



Check of critical system configuration including SAP system interfaces.



Vulnerability scan on OS, DB and SAP application level.



Scan of ABAP code for critical pattern.



Inventory and quality/security scan of RFC/http interfaces.

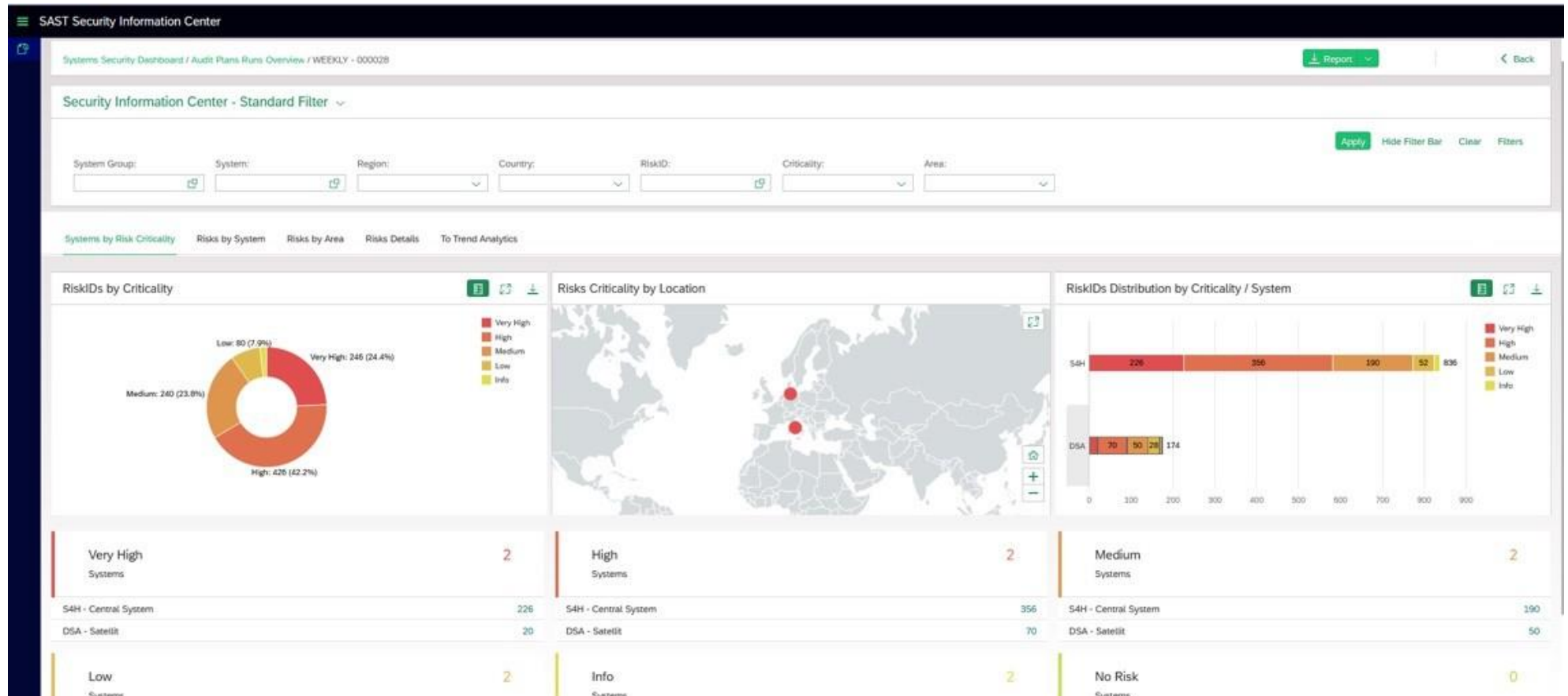


RFC/http interface optimization.

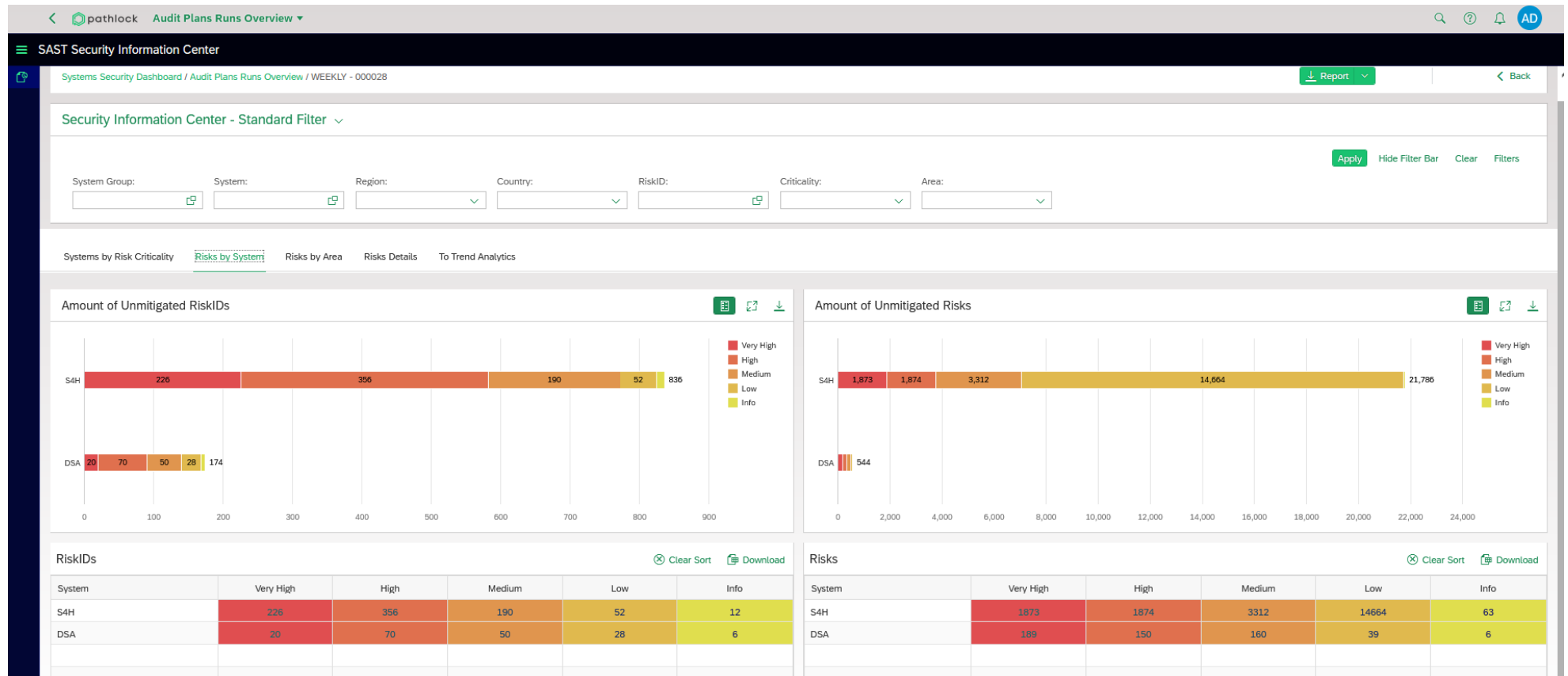


Get full transparency of communication relationships.

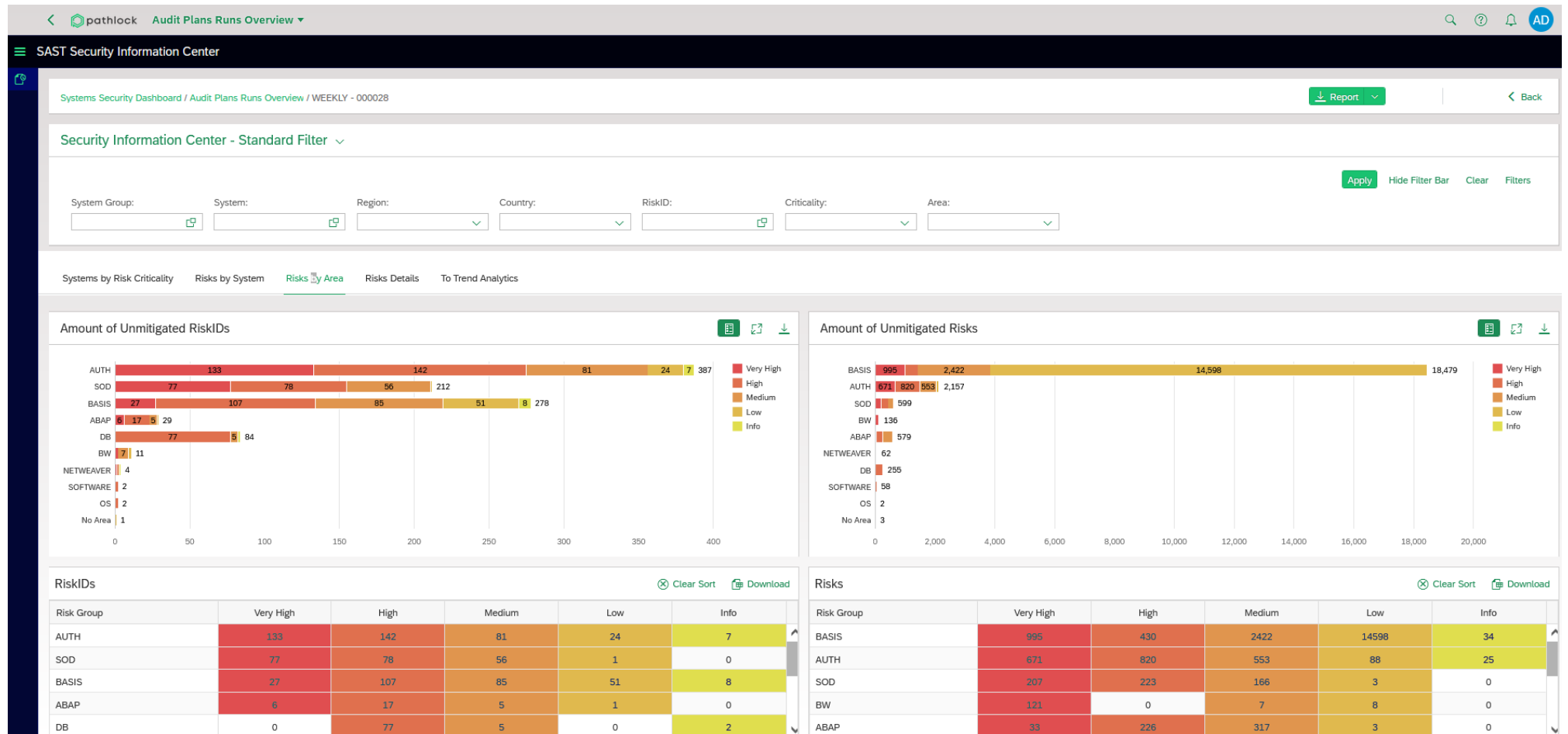
SAP Security Information Center



SAP Security Information Center



SAP Security Information Center



SAP Security Information Center

pathlock Audit Plans Runs Overview

SAST Security Information Center

Systems Security Dashboard / Audit Plans Runs Overview / WEEKLY - 000028

Report

Back

Security Information Center - Standard Filter

System Group:

System:

Region:

Country:

RiskID:

Criticality:

Area:

Apply

Hide Filter Bar

Clear

Filters

Systems by Risk Criticality
Risks by System
Risks by Area
Risks Details
To Trend Analytics

Risks Details

Clear Sort
Download

SystemID	Check Type	Description	RiskID	Area	Criticality	Risks Amount	Mitigated Risks	Remaining Risks
DSA	Critical auth.	Authorization to start / stop work processes	AUTH_00085	AUTH	Very High	1	0	1
DSA	Critical auth.	BC: S_DATASET Write or delete on all files possible	AUTH_00180	AUTH	Very High	3	0	3
DSA	Critical auth.	BC-USR - Create or change user via RFC (Groups SUSK and SU_USER)	AUTH_00238	AUTH	Very High	2	0	2
DSA	TSE	BW: User with all reporting authorizations (OBI_ALL)	BW__00008	BW	Very High	12	0	12
DSA	TSE	Table logging deactivated	PARAM00021	BASIS	Very High	1	0	1
DSA	TSE	Security Audit Log is deactivated	PARAM00025	BASIS	Very High	1	0	1
DSA	TSE	Secure Network Communication not active	PARAM00056	BASIS	Very High	1	0	1
DSA	TSE	File "REGINFO.DAT" not maintained	RFC__00008	BASIS	Very High	1	0	1
DSA	TSE	File "PROXY_INFO.DAT" not maintained	RFC__00020	BASIS	Very High	1	0	1
DSA	Critical auth.	The user has all SAP authorizations	SAP_ALL	AUTH	Very High	16	0	16

Showing results: 1-10 of 1010

Start
Previous
Next
End

SAP Security Information Center

