

Der blinde Fleck SAP – so schließen wir die Sicherheitslücke

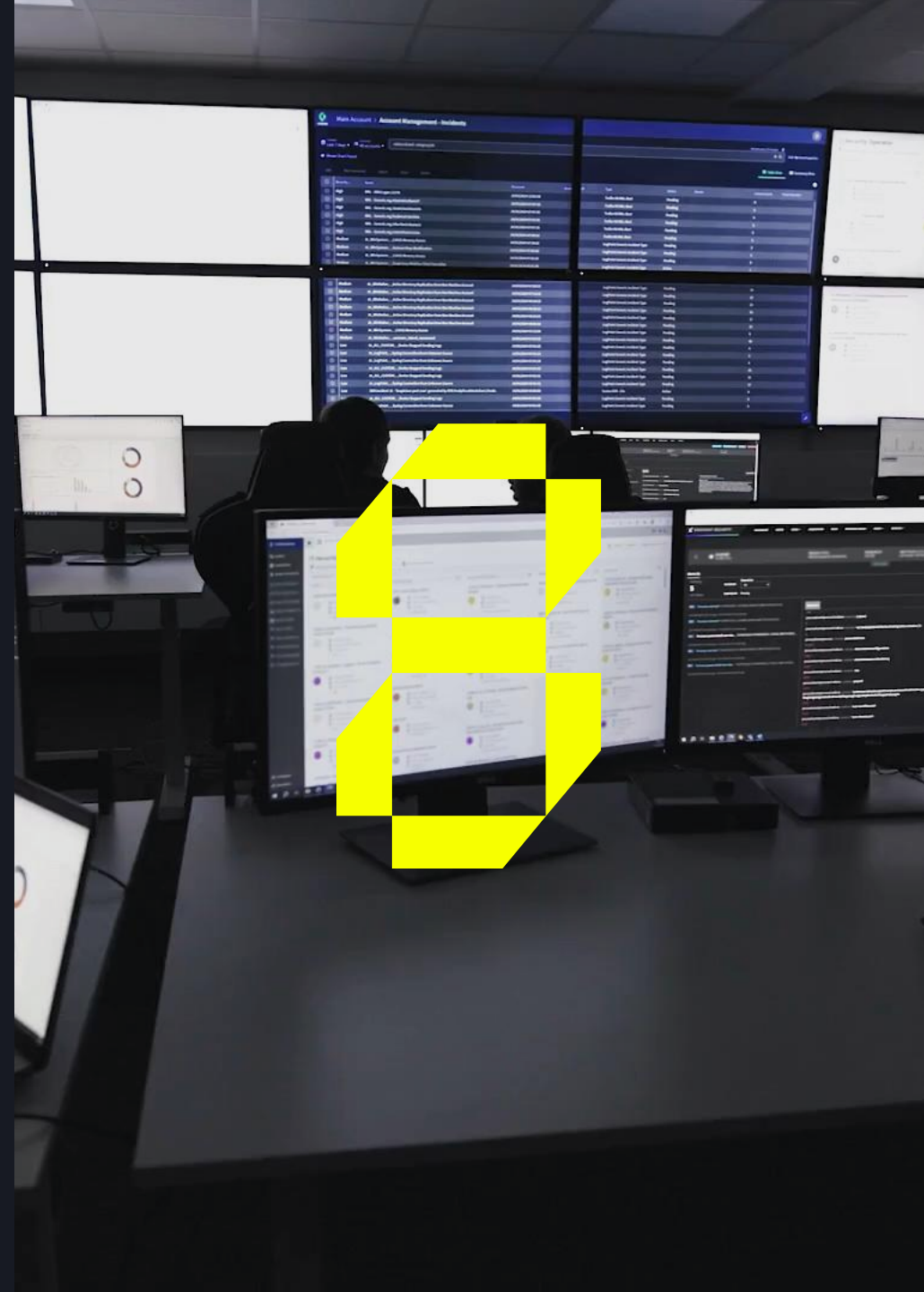
8COM
CYBER SECURITY

Eine Frage an Sie...

Ist SAP ein Baustein in Ihrer
zentralen IT-Security?

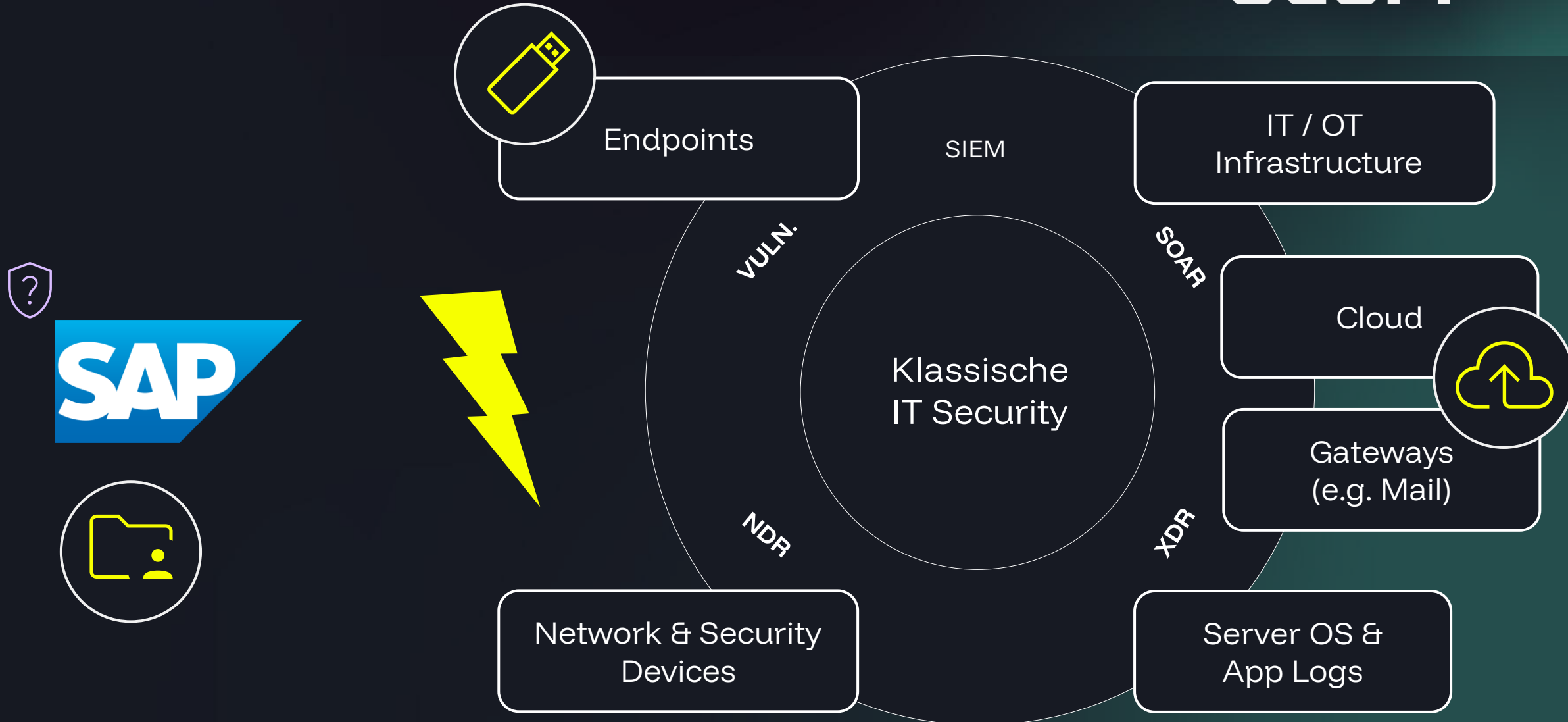
... kann Ihr SOC „SAP“?

8COM
CYBER SECURITY



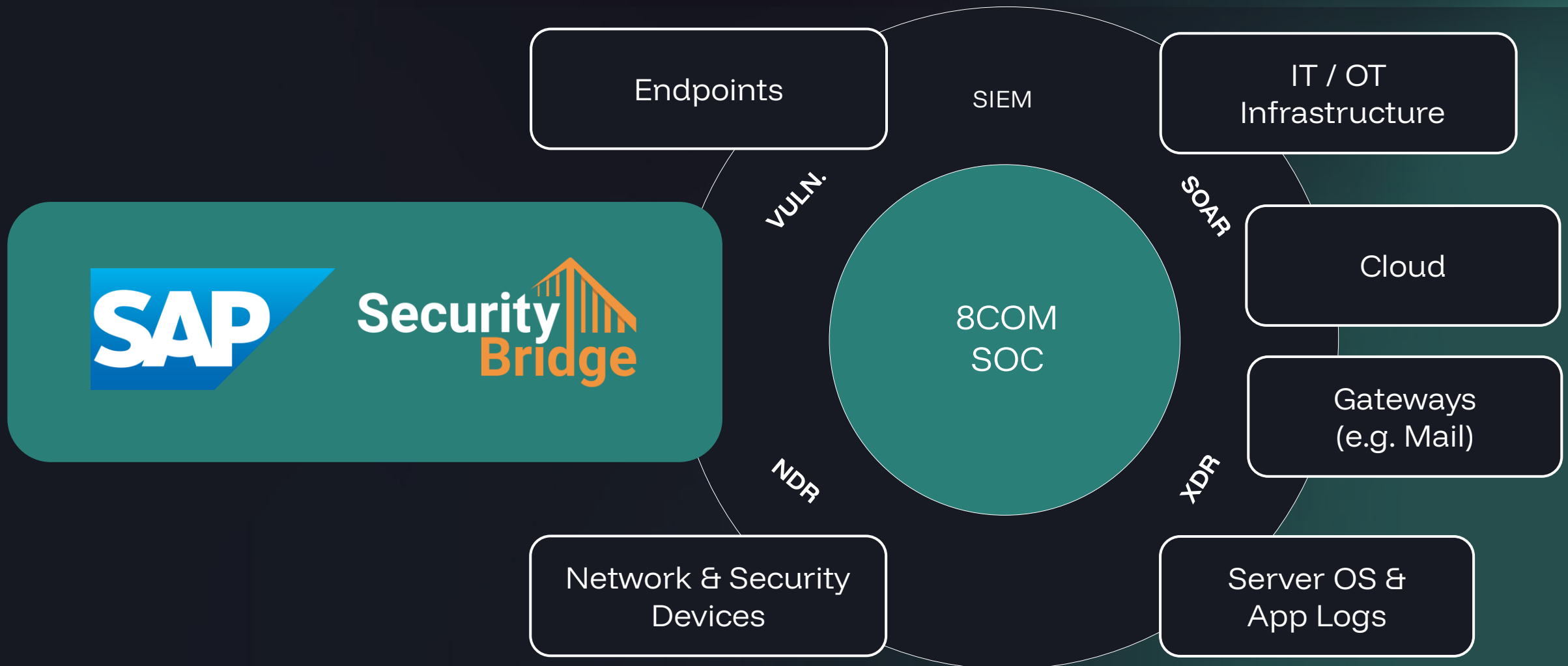
Der blinde Fleck SAP in der IT-Security

8COM



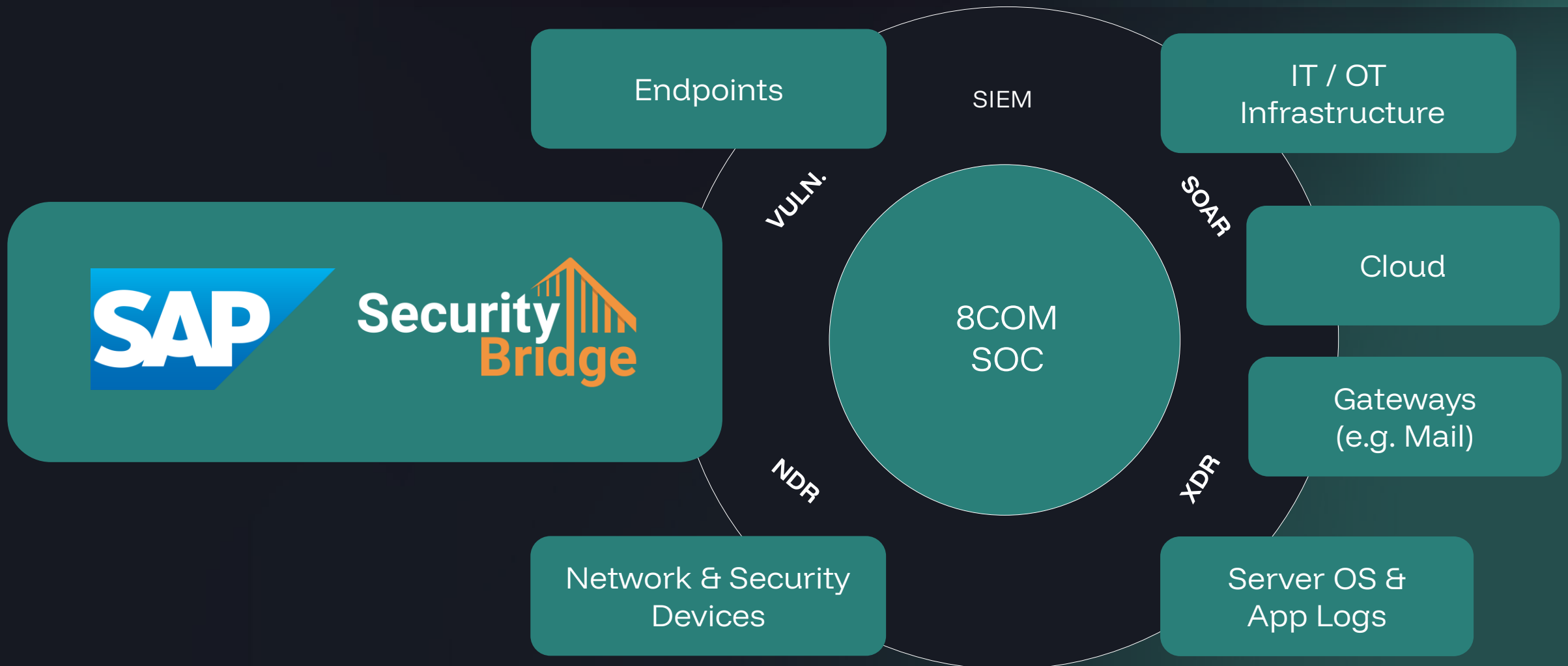
8COM eliminiert den blinden Fleck SAP

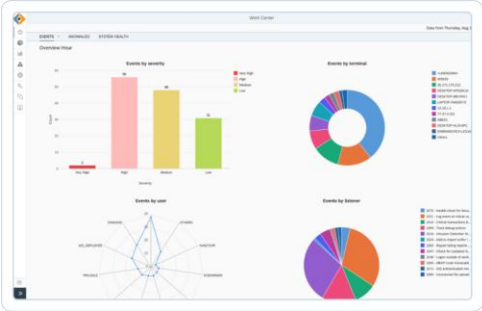
8COM



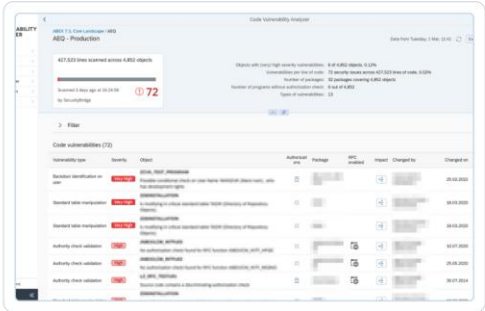
8COM eliminiert den blinden Fleck SAP

8COM



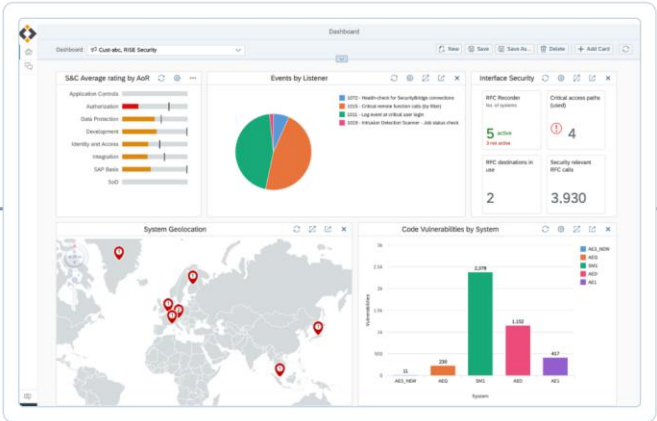


Threat Detection



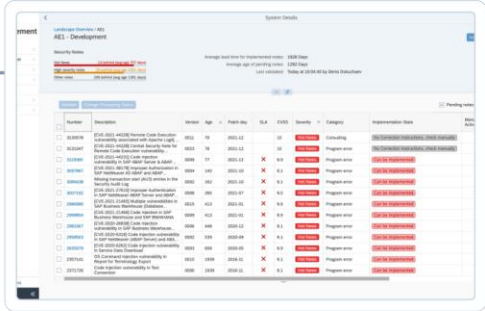
Code Vulnerability Scan

Security Management Dashboard

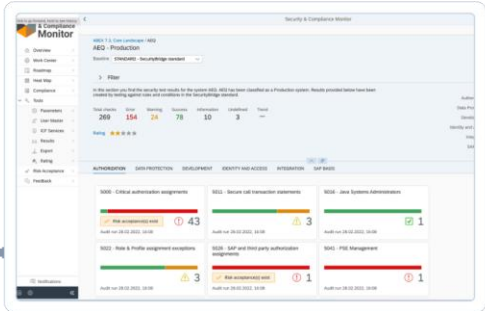


Assign Software Component and Namespace

- Integration with SAP S/4HANA
- Technical Uninstallation Test
- SAP Solution Manager Ready functionality
- Compatible with SAP S/4HANA Cloud, private edition
- Works with RISE with SAP



Patch Management

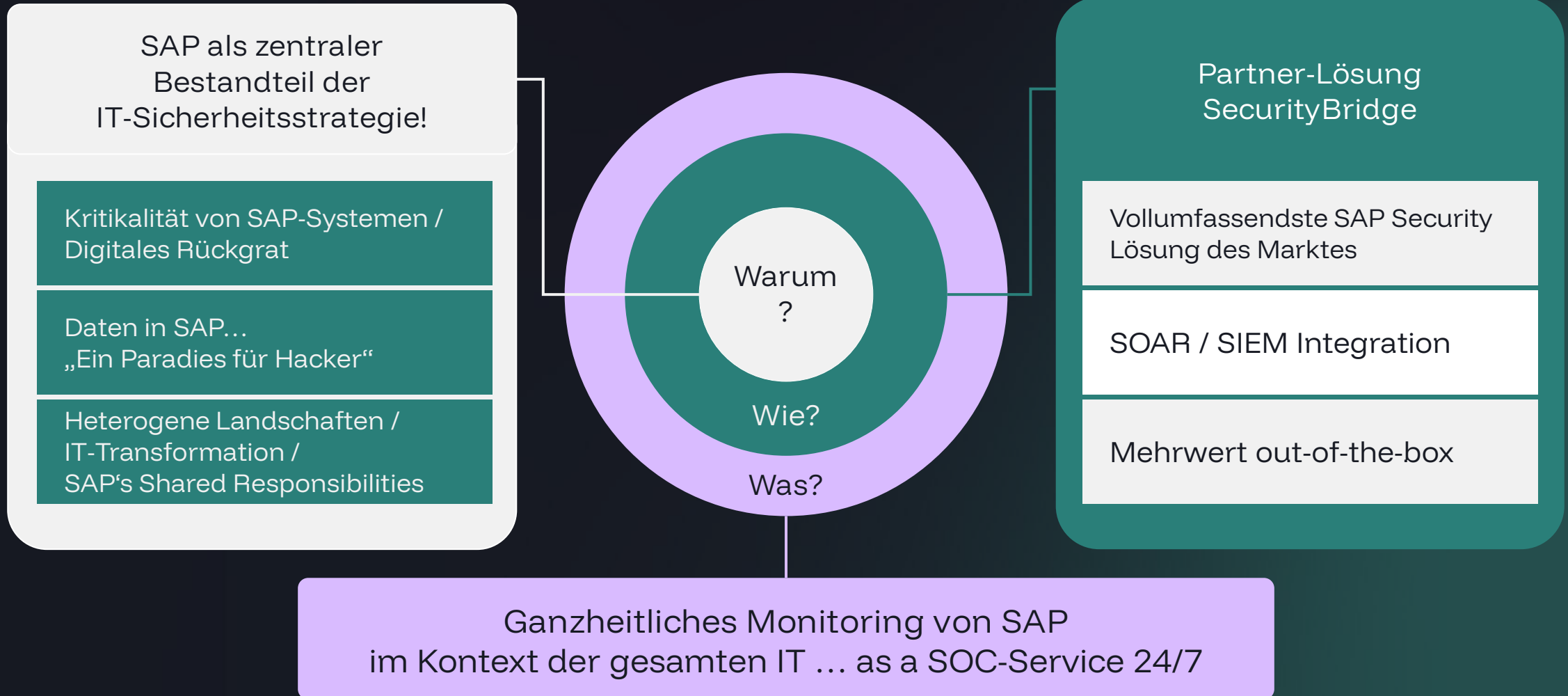


Security & Compliance



SAP im SOC-Fokus

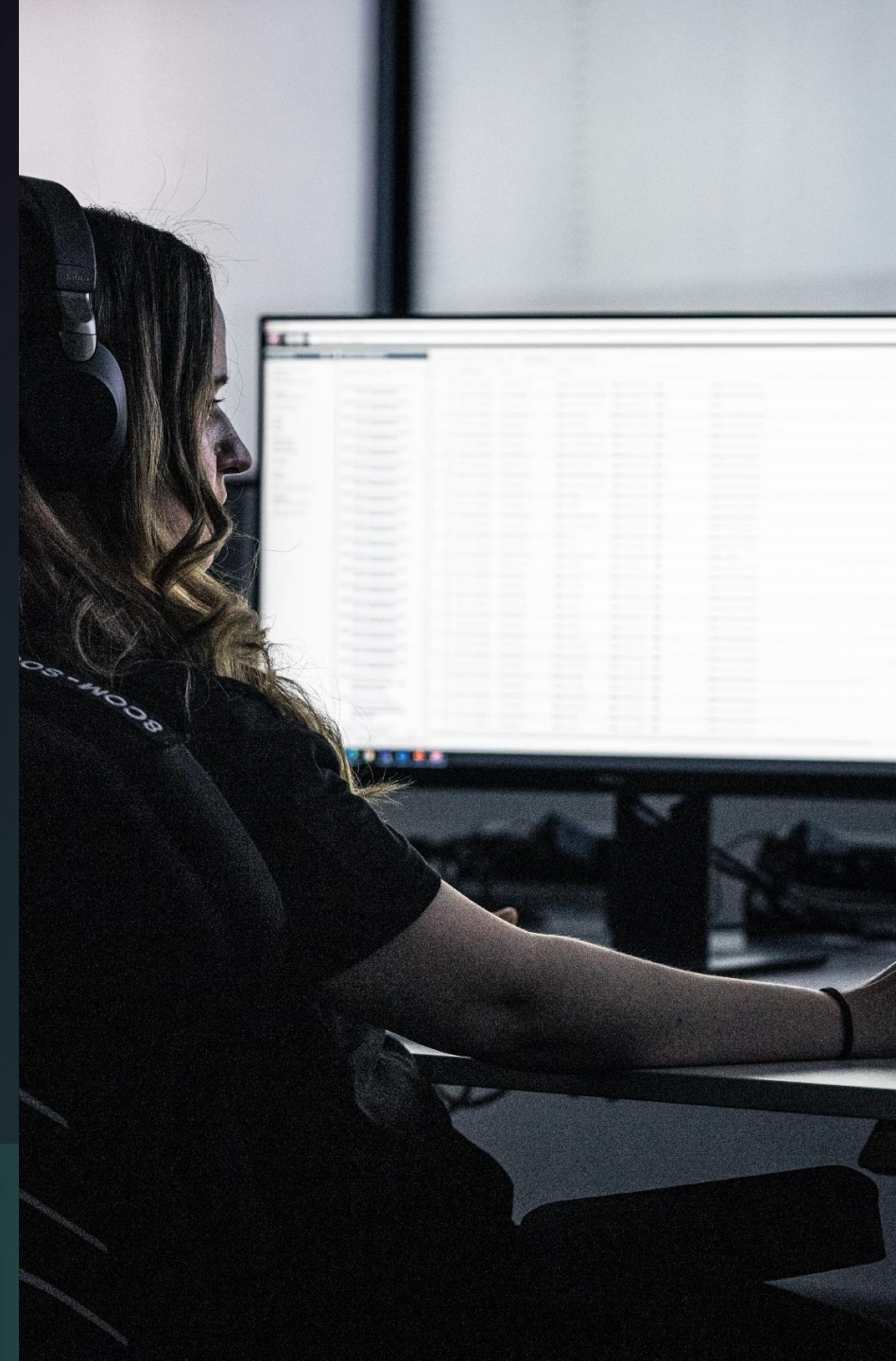
8COM



Der SOC-Mehrwert für SAP

- ✓ 8COM eliminiert den Blinden Fleck SAP in der IT-Security
 - ✓ Echtzeit-Monitoring - SAP Threat Detection 24/7/365
 - ✓ Vielzahl von Threat Detection-Szenarien - betriebsfertig
 - ✓ Schnelle Wertschöpfung und Steigerung des Sicherheitsniveaus
- ⇒ **SAP Security-Monitoring, wie es sein muss:**
KONTINUIERLICH.
AUTOMATISIERT.
GANZHEITLICH...
IM SOC!

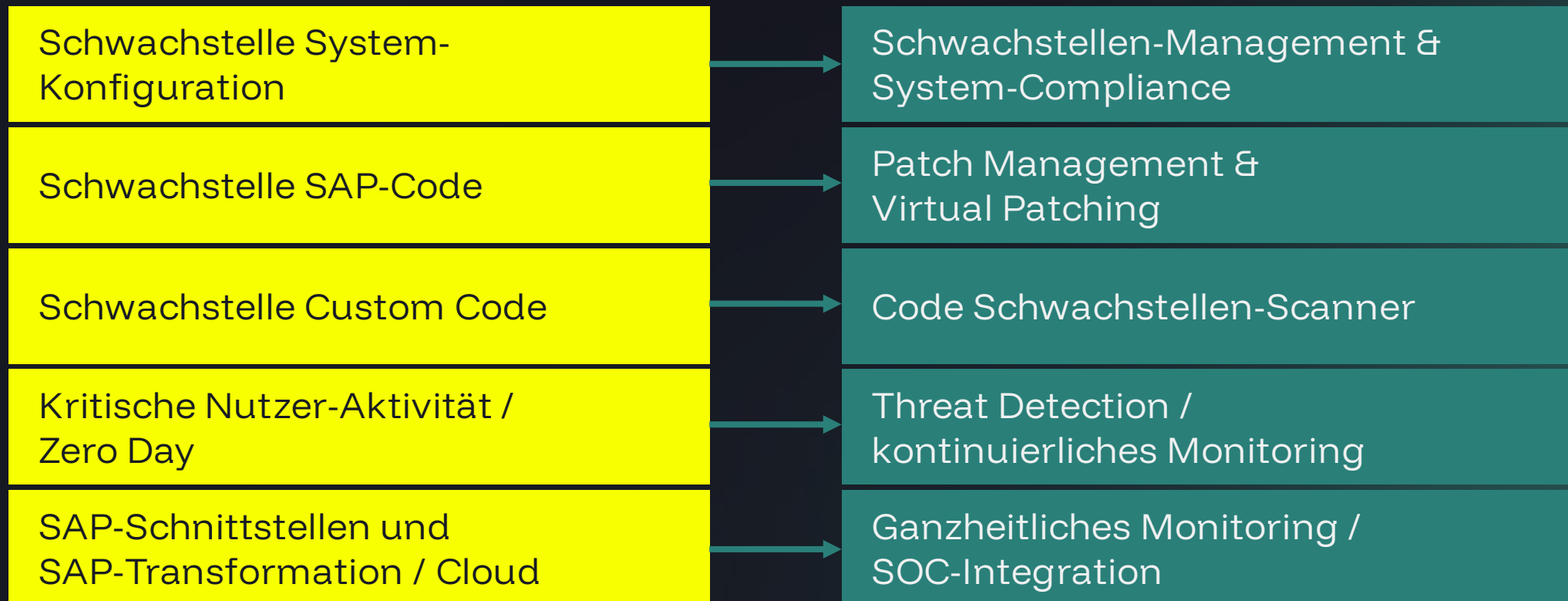
8COM



Vielen Dank für Ihre
Aufmerksamkeit!

8COM
CYBER SECURITY

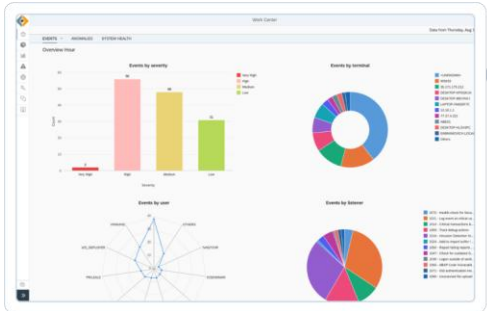
SAP-Angriffsvektoren & Lösungsbausteine



SecurityBridge – das Beste für zwei Welten!

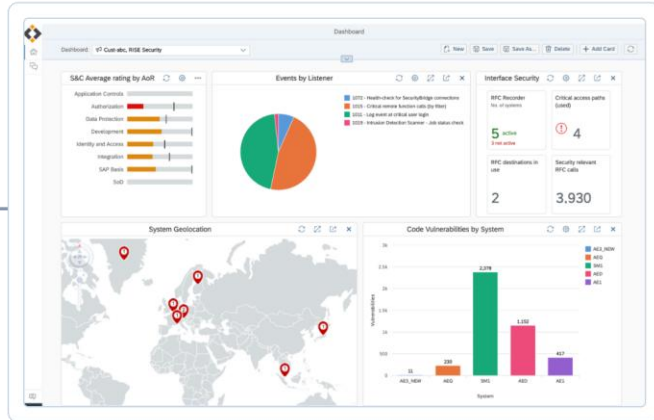
8COM





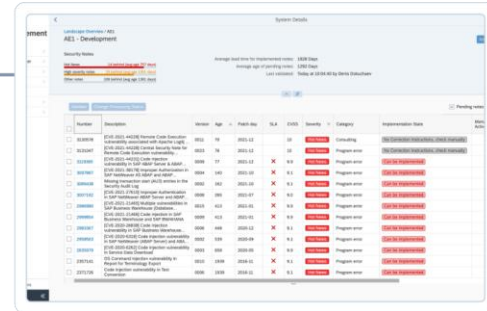
Threat Detection

Security Management Dashboard

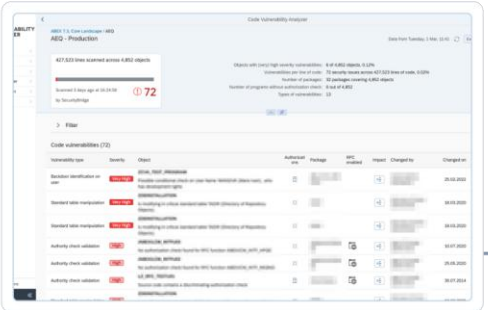


Assign Software Component and Namespace

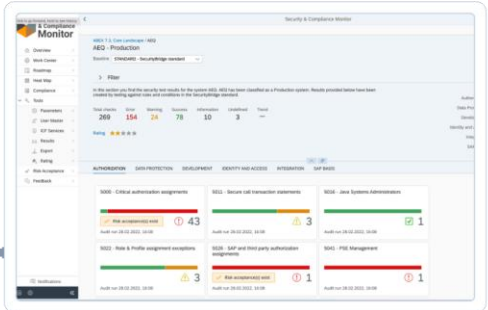
- Integration with SAP S/4HANA
- Technical Uninstallation Test
- SAP Solution Manager Ready functionality
- Compatible with SAP S/4HANA Cloud, private edition
- Works with RISE with SAP



Patch Management



Code Vulnerability Scan



Security & Compliance



Problem Description

Despite protection through secure configuration, timely installation of patches and the elimination of vulnerabilities in customer programs, there is still a risk of a zero-day attack. Such an attack can be detected by evaluating security-relevant incidents in the available SAP logs.

Solution

- **Real-time scanning** of all relevant SAP logs for suspicious activities
- Creation of **normalized events** with **decision enabling information**
- Intuitive **reporting** and **incident investigation** tools
- Option to **connect to SIEM**

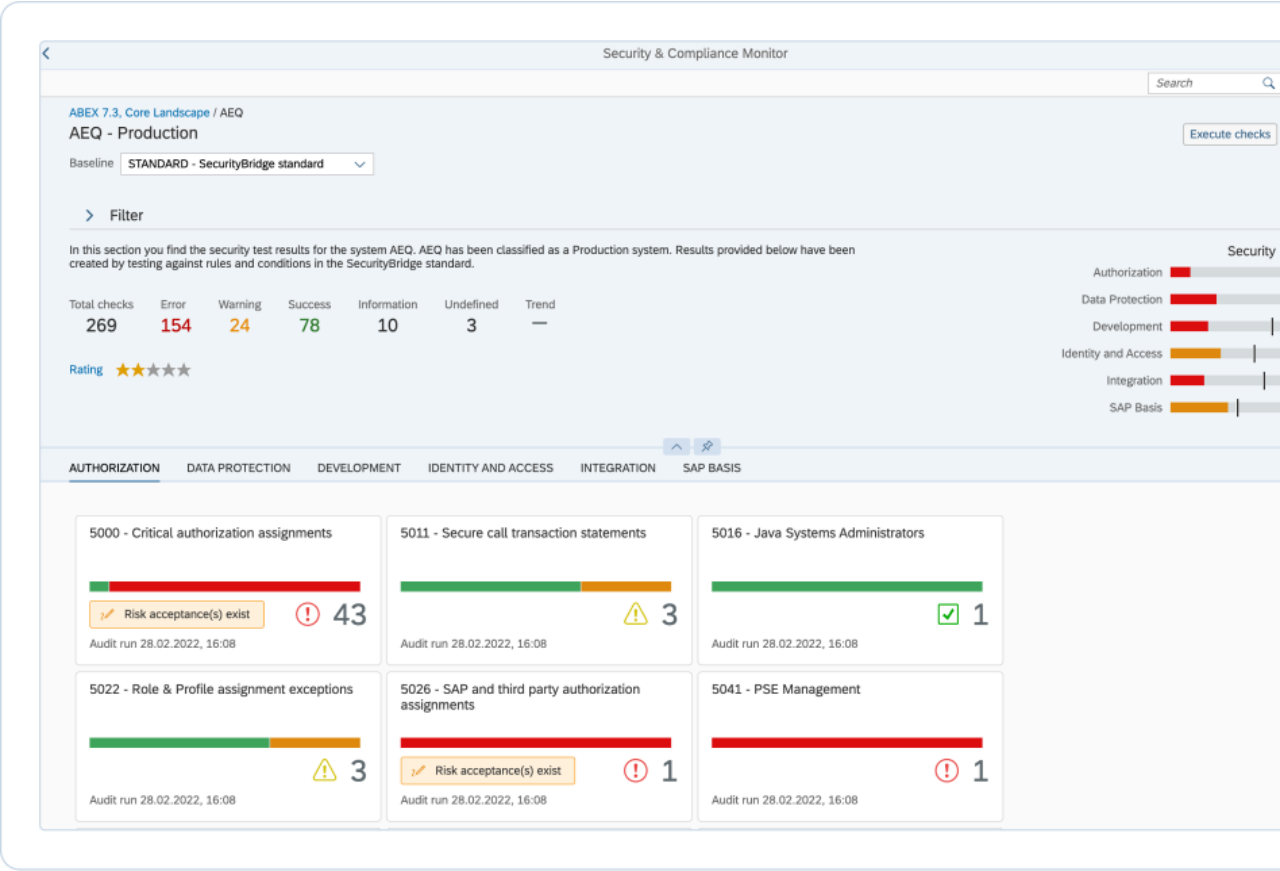


Problem Description

SAP NetWeaver and S/4HANA are complex enterprise applications that come with a wide range of config options. This complexity increases the risk of configuration vulnerabilities.

Solution

- **Continuous monitoring** of the security-relevant configuration
- **Multiple parallel Baselines:** SAP Security Recommendations, DSAG Security Audit Guide, SecurityBridge Baseline, Custom Baselines (project experience)
- **Integrated risk acceptance** and **incident management**



Problem Description

Known security issues in SAP SE products can be exploited by internal and external attackers. Exploits can be found on the Internet (e.g., Github) shortly after publication.

Solution

- Receive **precise information of available and relevant security updates/patches**
- SLA for **"time-to-patch"** based on priority
- Optimized operation through **360° view - available patches to relevant systems**
- **Integration** with Security & Compliance Monitor

System Details

Landscape Overview / AE1

AE1 - Development

Security Notes

Hot News14 behind (avg age 757 days)

High severity notes25 behind (avg age 1351 days)

Other notes106 behind (avg age 1361 days)

Average lead time for implemented notes: 1828 Days

Average age of pending notes: 1292 Days

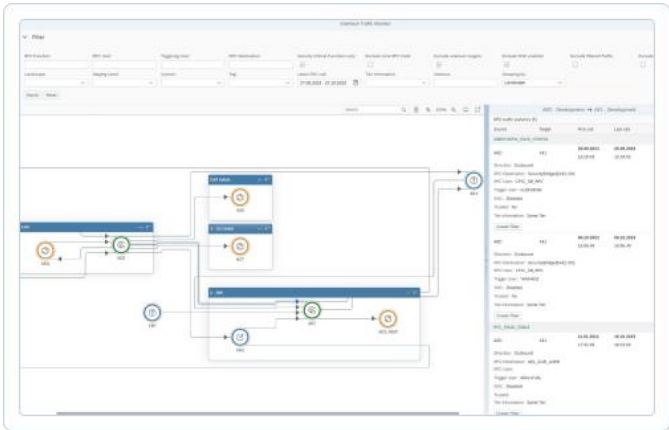
Last validated: Today at 10:04:40 by Denis Dokuchaev

ValidateChange Processing Status

☒ Pending

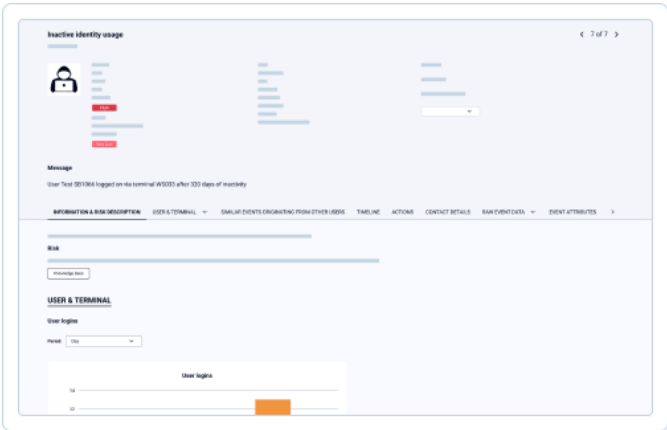
☐	Number	Description	Version	Age	Patch day	SLA	CVSS	Severity	Category	Implementation State
☐	3130578	[CVE-2021-44228] Remote Code Execution vulnerability associated with Apache Log4j ...	0011	70	2021-12		10	Hot News	Consulting	No Correction Instructions, check manually
☐	3131047	[CVE-2021-44228] Central Security Note for Remote Code Execution vulnerability...	0023	76	2021-12		10	Hot News	Program error	No Correction Instructions, check manually
☐	3119365	[CVE-2021-44231] Code Injection vulnerability in SAP ABAP Server & ABAP...	0009	77	2021-12	X	9.9	Hot News	Program error	Can be implemented
☐	3097887	[CVE-2021-38178] Improper Authorization in SAP NetWeaver AS ABAP and ABAP...	0004	140	2021-10	X	9.1	Hot News	Program error	Can be implemented
☐	3089438	Missing transaction start (AU3) entries in the Security Audit Log	0002	162	2021-10	X	9.1	Hot News	Program error	Can be implemented
☐	3007182	[CVE-2021-27610] Improper Authentication in SAP NetWeaver ABAP Server and ABAP...	0008	266	2021-07	X	9.0	Hot News	Program error	Can be implemented
☐	2986980	[CVE-2021-21465] Multiple vulnerabilities in SAP Business Warehouse (Database...	0015	413	2021-01	X	9.9	Hot News	Program error	Can be implemented
☐	2999854	[CVE-2021-21466] Code Injection in SAP Business Warehouse and SAP BW/4HANA	0009	413	2021-01	X	9.9	Hot News	Program error	Can be implemented
☐	2983367	[CVE-2020-26838] Code Injection vulnerability in SAP Business Warehouse...	0006	448	2020-12	X	9.1	Hot News	Program error	Can be implemented
☐	2958563	[CVE-2020-6318] Code Injection vulnerability in SAP NetWeaver (ABAP Server) and ABA...	0002	539	2020-09	X	9.1	Hot News	Program error	Can be implemented
☐	2835979	[CVE-2020-6262] Code Injection vulnerability in Service Data Download	0003	658	2020-05	X	9.9	Hot News	Program error	Can be implemented
☐	2357141	OS Command Injection vulnerability in Report for Terminology Export	0010	1939	2016-11	X	9.1	Hot News	Program error	Can be implemented
☐	2371726	Code Injection vulnerability in Text	0006	1939	2016-11	X	9.1	Hot News	Program error	Can be implemented

Has even more to offer...



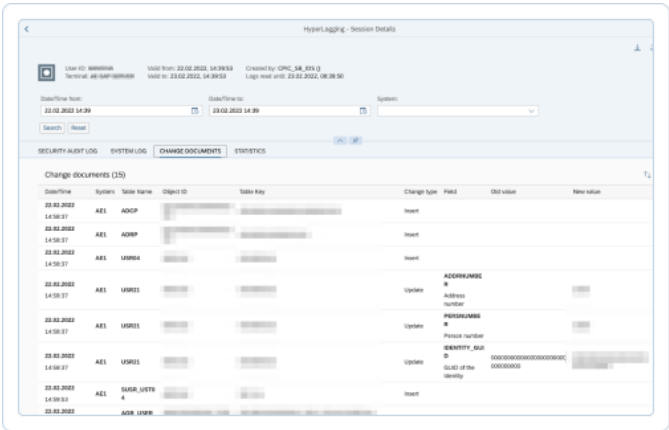
Interface Traffic

Graphical Interface Map: Finds security flaws within the integration layer of SAP applications.



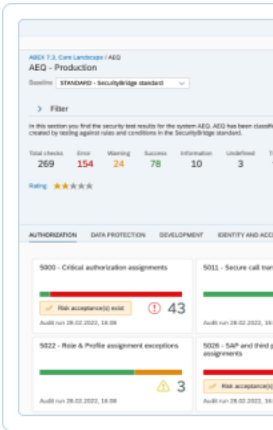
Identity protection

Prevent Identity Theft: Use state of the art protection approach to protect your SAP identities.



Transport Security

Scan Transport Content: Internal and external transport requests can be scanned for malicious content and vulnerable code.



And more...