



SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

**Risiko und Compliance Management mit der XAMS
heute und morgen – die Cloud im Visier**

Erik Trouillet | Olaf Sauer

Agenda

- 1. Heutige Anforderungen an ein GRC-Tool**
- 2. Wie setze ich die XAMS als GRC-Tool ein**
- 3. Der nächste Schritt: GRC in der Cloud**
- 4. Roadmap: Ein Ausblick**



Kapitel 1

Heutige Anforderungen an ein GRC-Tool

Was weiss ChatGPT über GRC?

ET Was sind die Anforderungen an ein GRC Tool?

Ein GRC-Tool (Governance, Risk, and Compliance-Tool) ist ein Software-Tool, das Unternehmen bei der Verwaltung und Überwachung von Governance-, Risiko- und Compliance-Aktivitäten unterstützt. Die Anforderungen an ein GRC-Tool können je nach Unternehmen und Branche unterschiedlich sein, aber im Allgemeinen sollten GRC-Tools folgende Funktionen und Eigenschaften haben:



Governance-
Unterstützung



Risikomanagement



Compliance-
Management



Reporting- und
Analysefähigkeiten



Benutzer-
freundlichkeit



Integration



Sicherheit



Skalierbarkeit

Quelle: OpenAI ChatGPT

Herausforderungen an die Sicherheit durch komplexe hybride Landschaften

Einheitliche Sicherheitsarchitektur für hybride Landschaften

- Einheitliche Konzepte
- Einheitliches Identitäten- und Berechtigungsmanagement
- Cross-System Segregation of Duties (auch Non-SAP)
- Einheitliches Security Monitoring
- Einheitlicher Umgang mit Threats



Kapitel 2

Wie setze ich die XAMS als GRC-Tool ein

GRC Funktionen in der XAMS und XCW



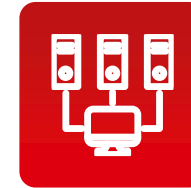
Regelwerk



Analyse



**Role
Management**



**User
Management**



**Rezertifizierung &
Betrieb**

SAP Cloud Identity Access Governance

SAP GRC Access Control

XAMS

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Identity Management

XCW

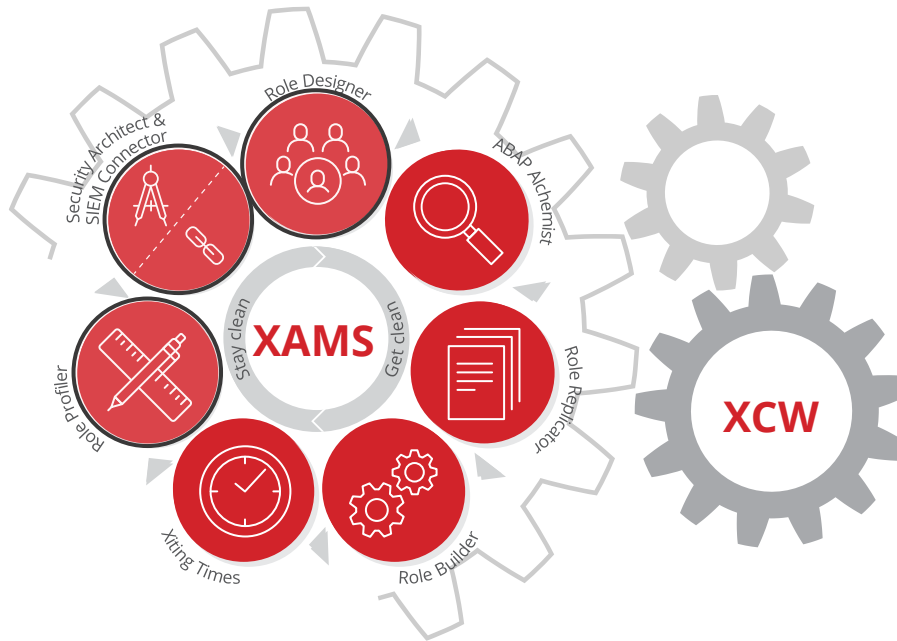
XAMS



Risikoanalyse mit XAMS CRAF

Critical Authorization Framework

Das CRAF ist die Schaltzentrale der XAMS, welche Prüfungsmöglichkeiten zu jeder Zeit erlaubt.



XAMS CRAF ist in mehreren XAMS Modulen nativ integriert:

1. Role Designer für die Prüfung von virtuellen Rollen noch vor Erstellung in PFCG
2. Role Profiler zur Qualitätssicherung (Adhoc Analysen)
3. Security Architect für regelmässige Risikoanalysen (Controls Monitoring)

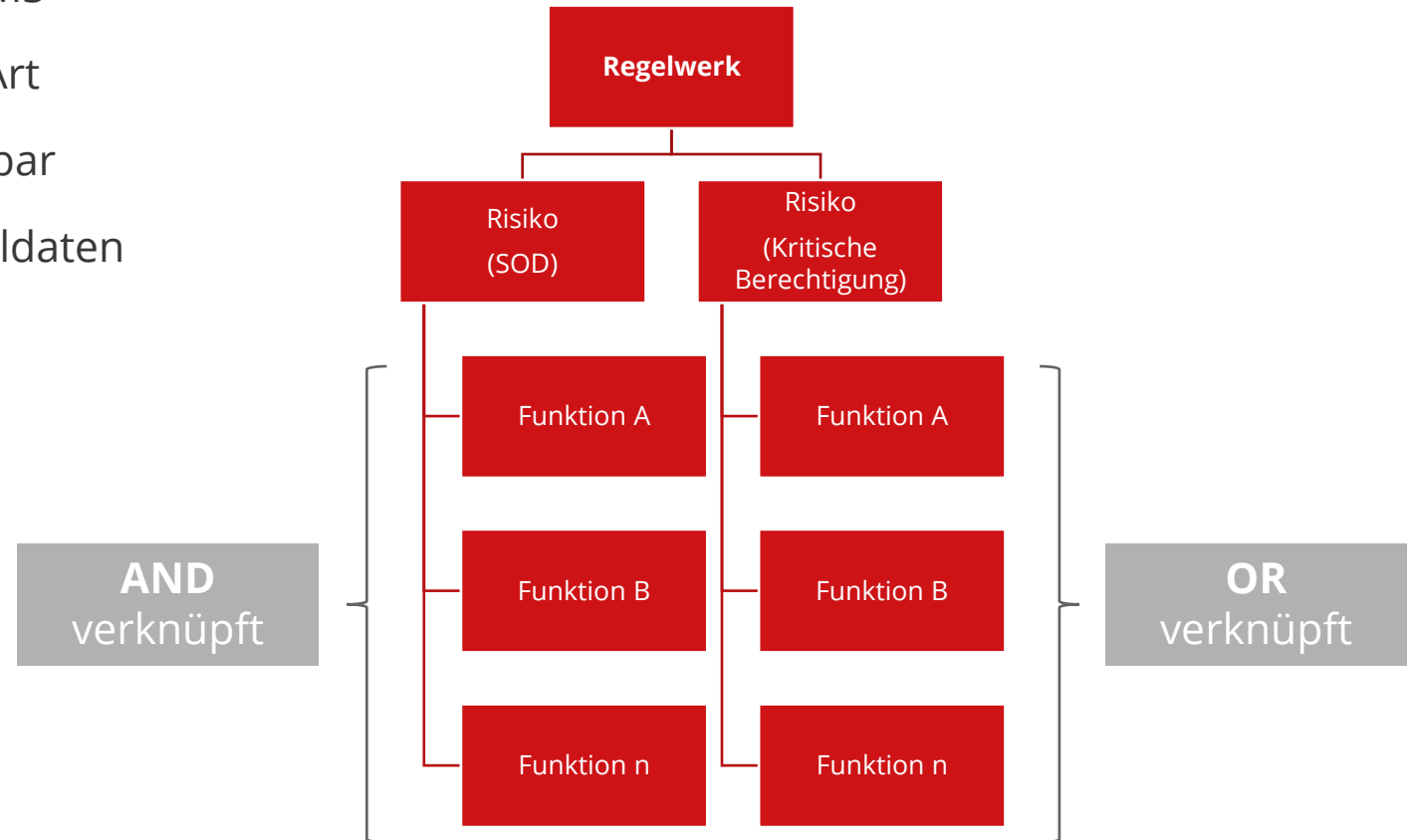
Sowie im "SAP Standard" bei Bedarf:

4. PFCG zur Direktprüfung bei Rollenänderungen



Critical Authorizations Framework

- Zentrales Prüfungs-Framework in der XAMS
- Risikoanalyse mit Hilfe von Regeln jeder Art
- Jede Komplexität ist bei den Regeln denkbar
- Prüfungsgrundlage sind Rollen- und Profildaten
- Zentrale Überwachungsmöglichkeiten
- Vielseitige Integration
- Mitigationsframework



SOD Prüfung auf Ebene Rollen und / oder Benutzer

Xiting Role Profiler: Kritische Rollen Kombinationen (17 hits)

Selektion Vollbild an/aus Aktualisieren Berechtigungsdaten Berechtigungsdaten Rolle ↔ Rolle Inspektion Mitigation Dokumentation

Variantenbeschreibung Customizing Andere Variante überprüfen

Role Profiler Berichte
 • Favoriten
 ▾ Role Profiler Berichte
 ▸ Rollenqualität
 ▸ Abgeleitete Rollen Berichte
 ▸ Rollentransport
 ▸ Rollencustomizing
 ▸ SU24 Optimierungsreports
 ▸ Mitigations-Berichte
 ▸ Rollenmenüprüfungen
 ▸ ST03N Auswertungen
 ▸ Benutzer Reports
 ▾ "Watchdog" Berichte für Rollen
 • Anzeigerollen Watchdog
 • Stammdatenpflege Watchdog
 • Bewegungsdatenbuchen Watchdog
 • HR-Zuarriff Rollen Watchdog
 • **Kritische Rollen Berechtigung**
 • **Kritische Berechtigungen - GRC**
 • **Kritische Rollen Kombinationen**
 • Kritische Kombinationen - GRC
 • Voll Funktionalität Watchdog
 • Berechtigungswerte Watchdog
 ▸ **"Watchdog" Berichte für User**
 ▸ CRAF ID Mapping zu Cloud-Berechtigung

Mit.	Rollentyp	Rolle	Fehlerzahl	Bezeichnung der Rolle
		Z_FI_DEBITOR	1	*** NEW ***
		Z_FI_DEBITOR0001	2	*** NEW ***
		Z_FI_DEBITOR1	2	*** NEW ***
		Z_FI_DEBITOR_CH	2	Vorlage Z_FI_DEBITOR repliziert für Orgset X-CH
		Z_FI_DEBITOR_DE	2	Vorlage Z_FI_DEBITOR repliziert für Orgset X-DE
		Z_FI_DEBITOR_EUROPE	2	Vorlage Z_FI_DEBITOR repliziert für Orgsetgruppe X_EUROPE
		Z_FI_DEBITOR_MARC_DE	2	Vorlage Z_FI_DEBITOR_TEMPLATE repliziert mit Orgset Orgset X-DE
		Z_FI_DEBITOR_NONEUROPE	2	Vorlage Z_FI_DEBITOR repliziert für Orgsetgruppe X_NONEUROPE
		Z_FI_DEBITOR_RO	2	Vorlage Z_FI_DEBITOR repliziert für Orgset X-RO
		Z_FI_DEBITOR_SWE	2	Vorlage Z_FI_DEBITOR repliziert für Orgset X-SWE
		Z_FI_DEBITOR_TEMPLATE	2	
		Z_FI_DEBITOR_UK	2	Vorlage Z_FI_DEBITOR repliziert für Orgset X-UK
		Z_FI_DEBITOR_US	2	Vorlage Z_FI_DEBITOR repliziert für Orgset X-US
		Z_FI_DEBITOR_XITING	2	Vorlage Z_FI_DEBITOR repliziert für Orgsetgruppe X-00
		Z_FI_DEBITOR_COMP	2	
		Z_ADM940_FI_DEBITOR	1	Einzelrolle für Finanzdebitoren
		Z_ADM940_FI_DEBITOR_KEYUSER	1	

Ergebnisse

Rolle	ID der kritischen Kombination	Konflikt	Text	Beschreib
Z_FI_DEBITOR_CH	/XITING/BC001	↔	Risiko: Basis -> Entwicklungstätigkeiten & Systemadmin&abdu	i
Z_FI_DEBITOR_CH	/XITING/BC002	↔	Risiko: Sicherheit -> Benutzer- & Berechtigungsverwaltung	i



Qualitative Beschreibung des SOD Konflikts

Ergebnisse

Mitigieren Aktualisieren

Rolle	ID der kritischen Kombination	Konflikt	Text	Beschreibung
Z_FI_DEBITOR_CH	/XITING/BC001	⚡	Risiko: Basis -> Entwicklungstätigkeiten & Systemadmin&abdu	i
Z_FI_DEBITOR_CH	/XITING/BC002	⚡	Risiko: Sicherheit -> Benutzer- & Berechtigungsverwaltung	i

Kritische Berechtigungen - GRC
Kritische Rollen Kombinationen
Kritische Kombinationen - GRC
Voll Funktionalität Watchdog
Berechtigungswerte Watchdog

Beschreibung der Kombinations-ID /XITING/BC001

Die Berechtigungen erlauben grundsätzliche Tätigkeiten in der Systemadministration und in Entwicklungsbereich. Durch die Kombination besteht die Möglichkeit zur Manipulation von Entwicklungsobjekte jeglicher Art und ermöglicht es Anpassungen auf der produktiven Umgebungen direkt vorzunehmen.



Technische Darstellung des SOD Konflikts

☞ Konflikte

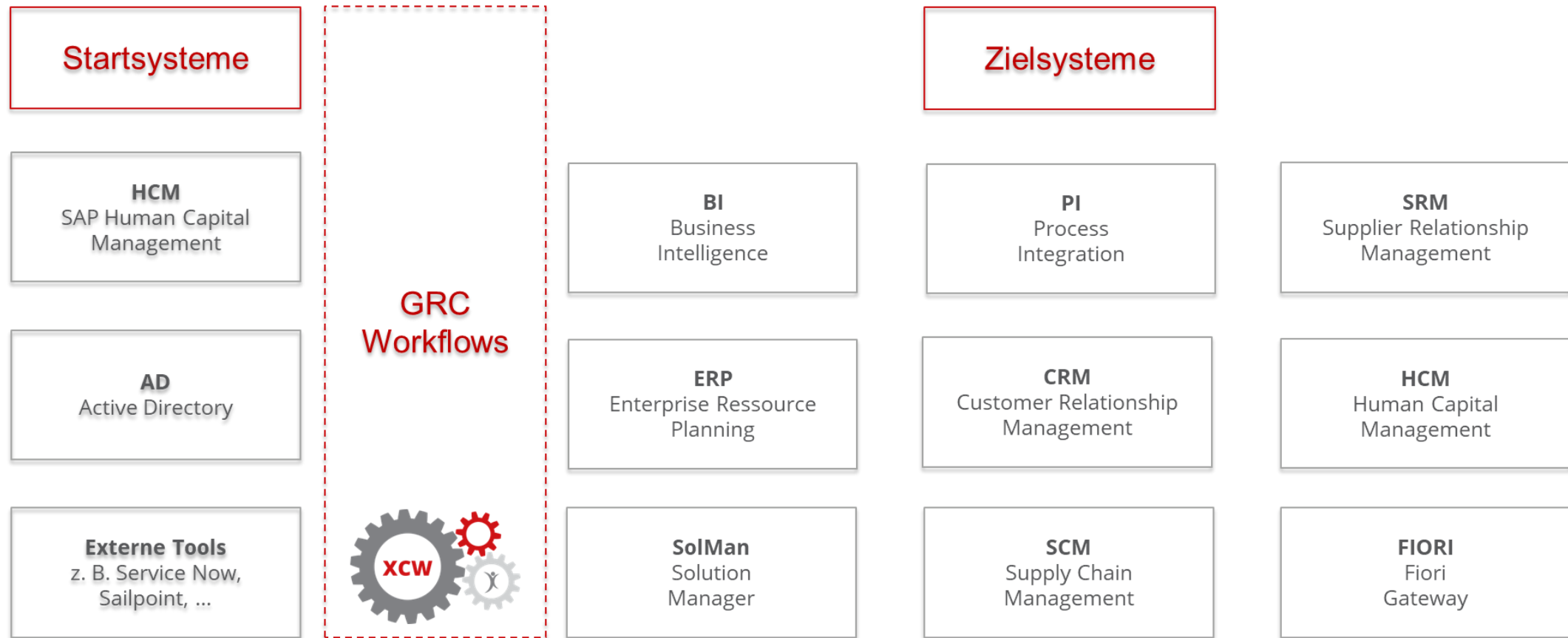
Rollenobjekt	Rollenauth.	Rollenfeld	Rolle-Von	Rolle-Bis	Status	Verwend.	Obj.Wer...	AuthID	Grup...
S_DEVELOP	T-XT6011970...	ACTVT	01					/XITING/BC_ADM1	ORG2
S_DEVELOP	T-XT6011970...	ACTVT	02					/XITING/BC_ADM1	ORG2
S_DEVELOP	T-XT6011970...	OBJTYPE	FUGR					/XITING/BC_ADM1	ORG2
S_RFC_ADM	T-XT6011970...	ACTVT	01					/XITING/BC_ADM2	OR1
S_RFC_ADM	T-XT6011970...	ACTVT	02					/XITING/BC_ADM2	OR1
S_RFC_ADM	T-XT6011970...	ACTVT	06					/XITING/BC_ADM2	OR1
S_USER_GRP	T-XT6011970...	ACTVT	06					/XITING/BC_ADM2	OR1
S_USER_GRP	T-XT6011970...	ACTVT	06					/XITING/BC_ADM2	OR1

☞ Beschreibung der Kombinations-ID /XITING/BC001

Die Berechtigungen erlauben grundsätzliche Tätigkeiten in der Systemadministration und in Entwicklungsbereich. Durch die Kombination besteht die Möglichkeit zur Manipulation von Entwicklungsobjekte jeglicher Art und ermöglicht es Anpassungen auf der produktiven Umgebungen direkt vorzunehmen.



Workflows für die Provisionierung / Entzug von Berechtigungen



Workflows für die Provisionierung / Entzug von Berechtigungen (Fortsetzung)

Benutzeranlage/-änderung

- Erstellung einer neuen SAP-Benutzerkennung
- Änderung einer bestehenden SAP-Benutzerkennung

Rollenvergabe/-entzug

- Zuweisung einer Rolle zu einer SAP-Benutzerkennung
- Entzug einer Rolle von einer SAP-Benutzerkennung

**GRC
Workflows**



Benutzeranlage inkl. Rollenvergabe

- Erstellung einer neuen SAP-Benutzerkennung inkl. Zuweisung von Rollen



Erfüllung der GRC Anforderungen mit der XAMS

- Die XAMS hat ihre Stärken im SAP Berechtigungsmanagement und nutzt diese für sämtliche GRC Funktionen.



Governance-
Unterstützung



Risikomanagement



Compliance-
Management



Reporting- und
Analysefähigkeiten



Benutzer-
freundlichkeit



Integration



Sicherheit



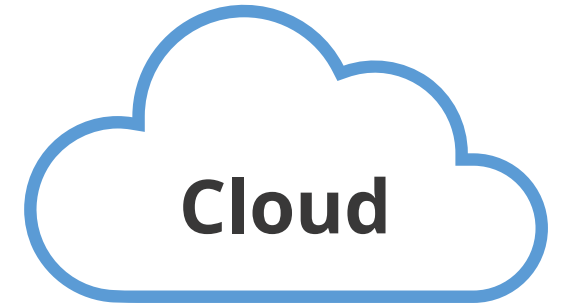
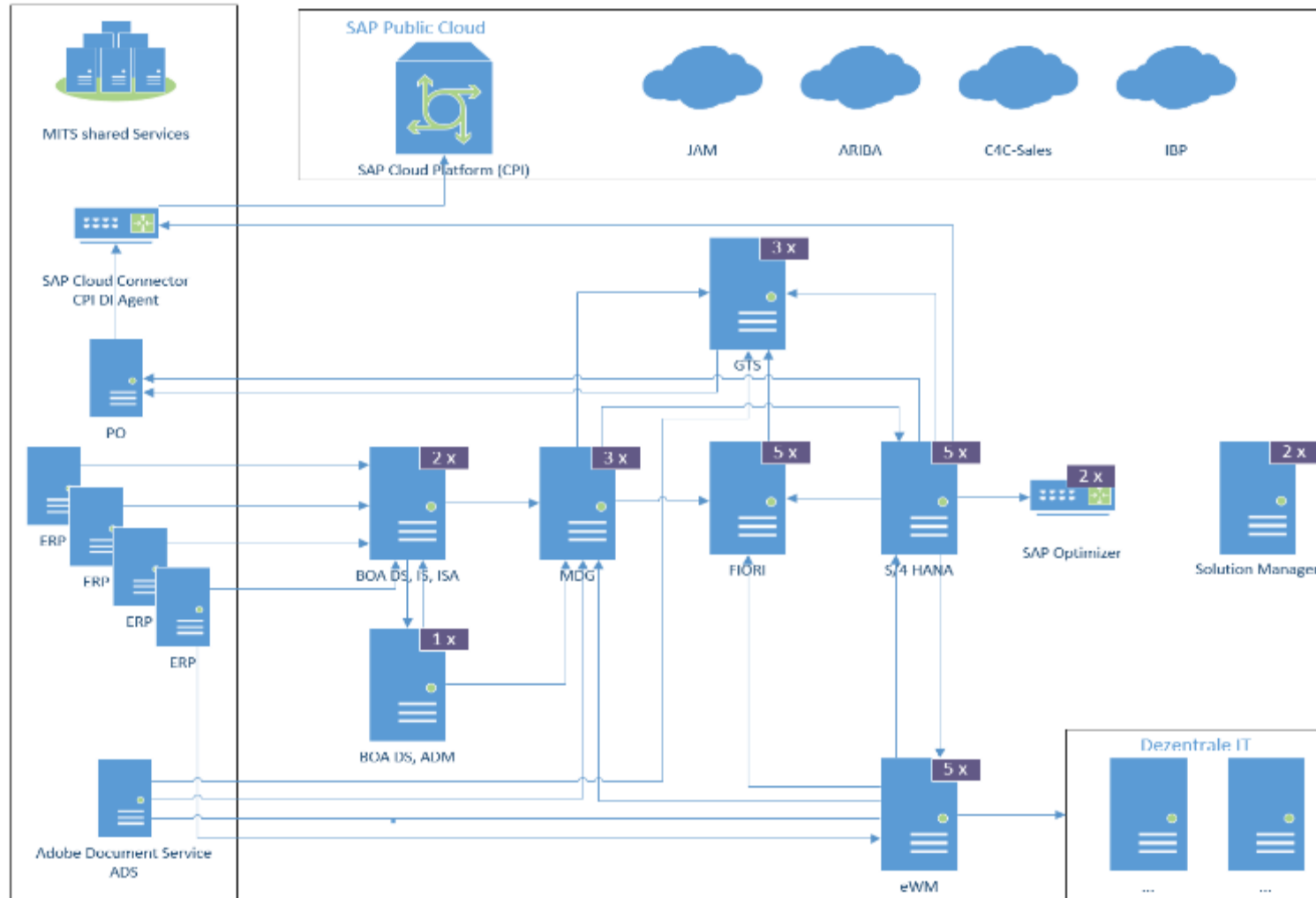
Skalierbarkeit



Kapitel 3

Der nächste Schritt: GRC in der Cloud

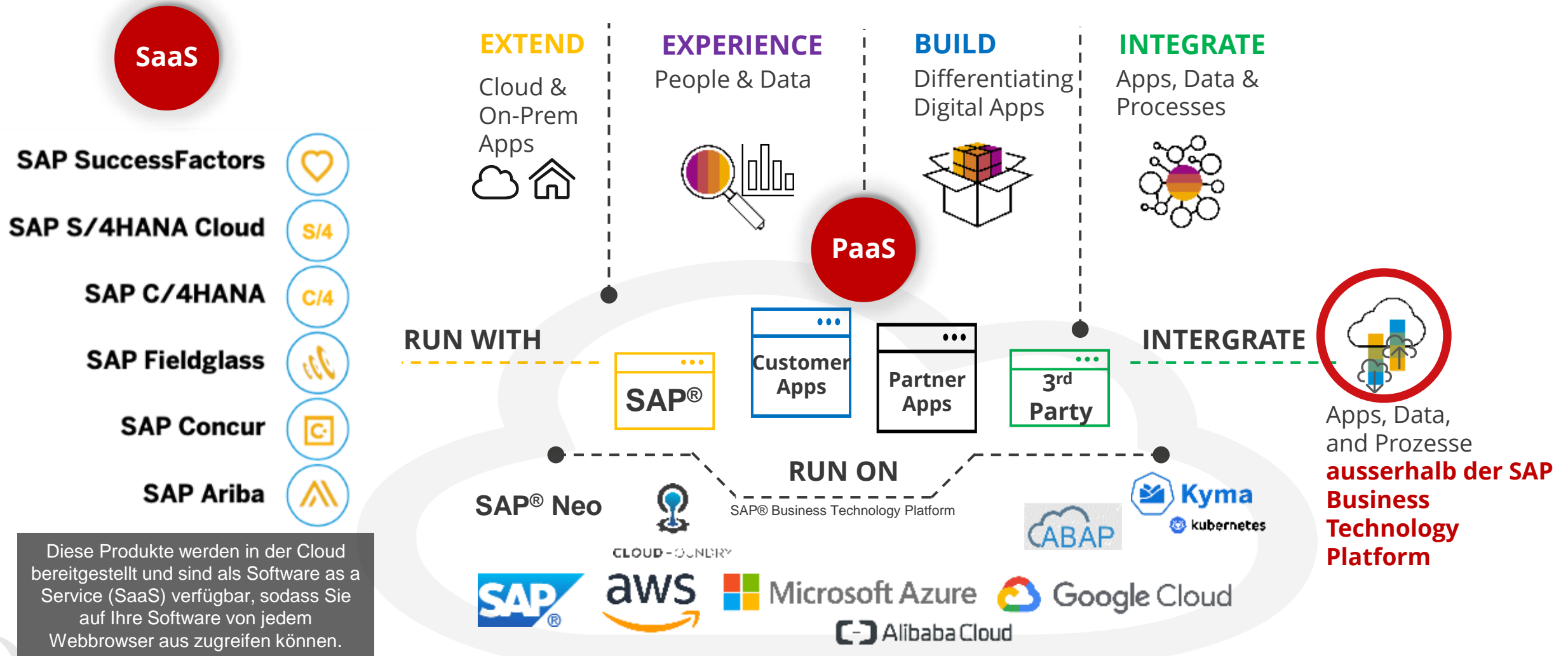
Komplexe hybride Landschaft Kundensicht



On-premise



Komplexe hybride Landschaft SAP-Sicht



Diese Produkte werden in der Cloud bereitgestellt und sind als Software as a Service (SaaS) verfügbar, sodass Sie auf Ihre Software von jedem Webbrowser aus zugreifen können.

GRC Funktionen aus der Cloud, für die Cloud, in der Cloud



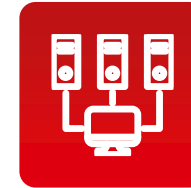
Regelwerk



Analyse



**Role
Management**



**User
Management**



**Rezertifizierung &
Betrieb**

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Cloud Identity Access Governance

SAP GRC Access Control

SAP Identity Management

XAMS

XCW

XAMS

XSP

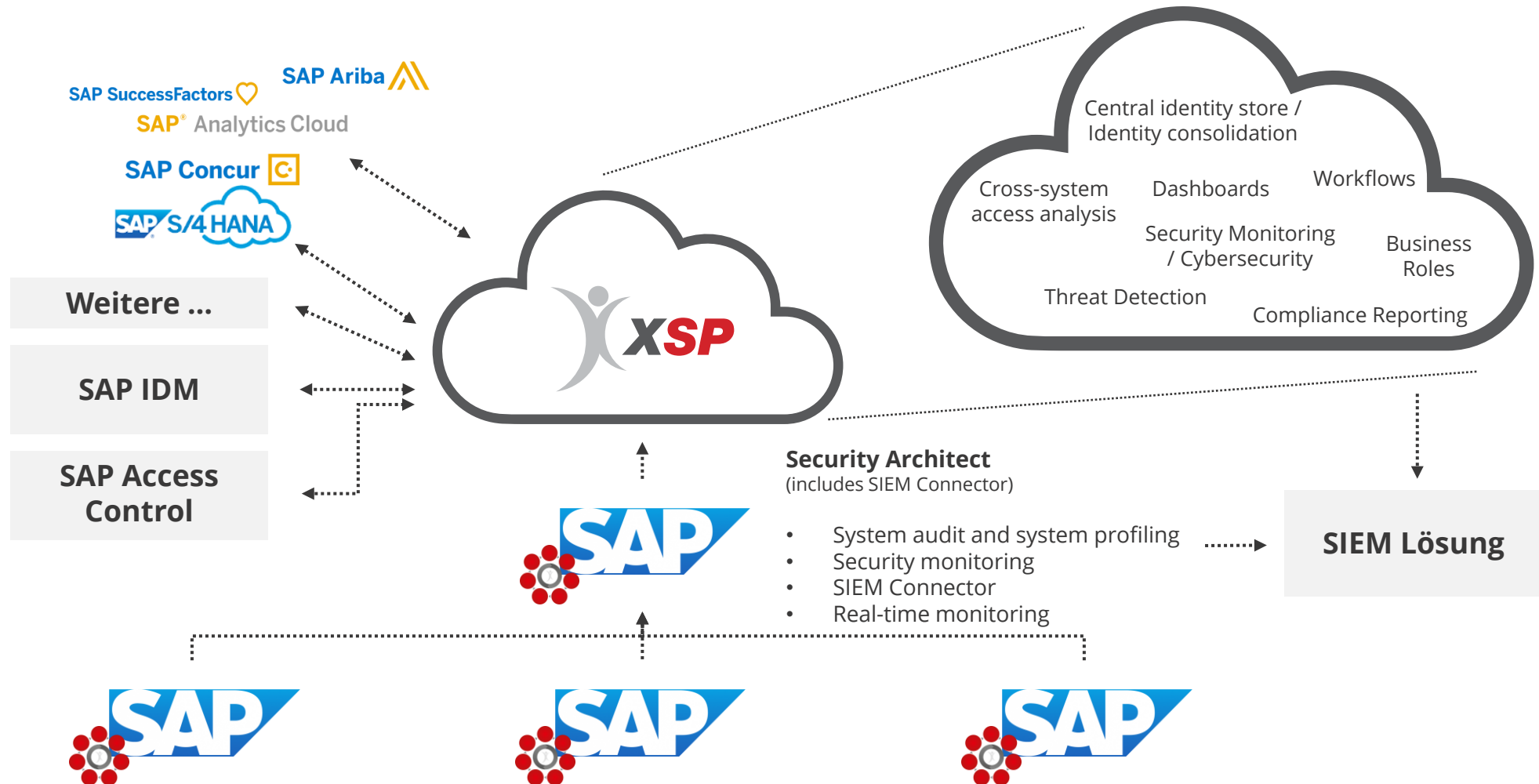
XSP (Business Roles)

XSP

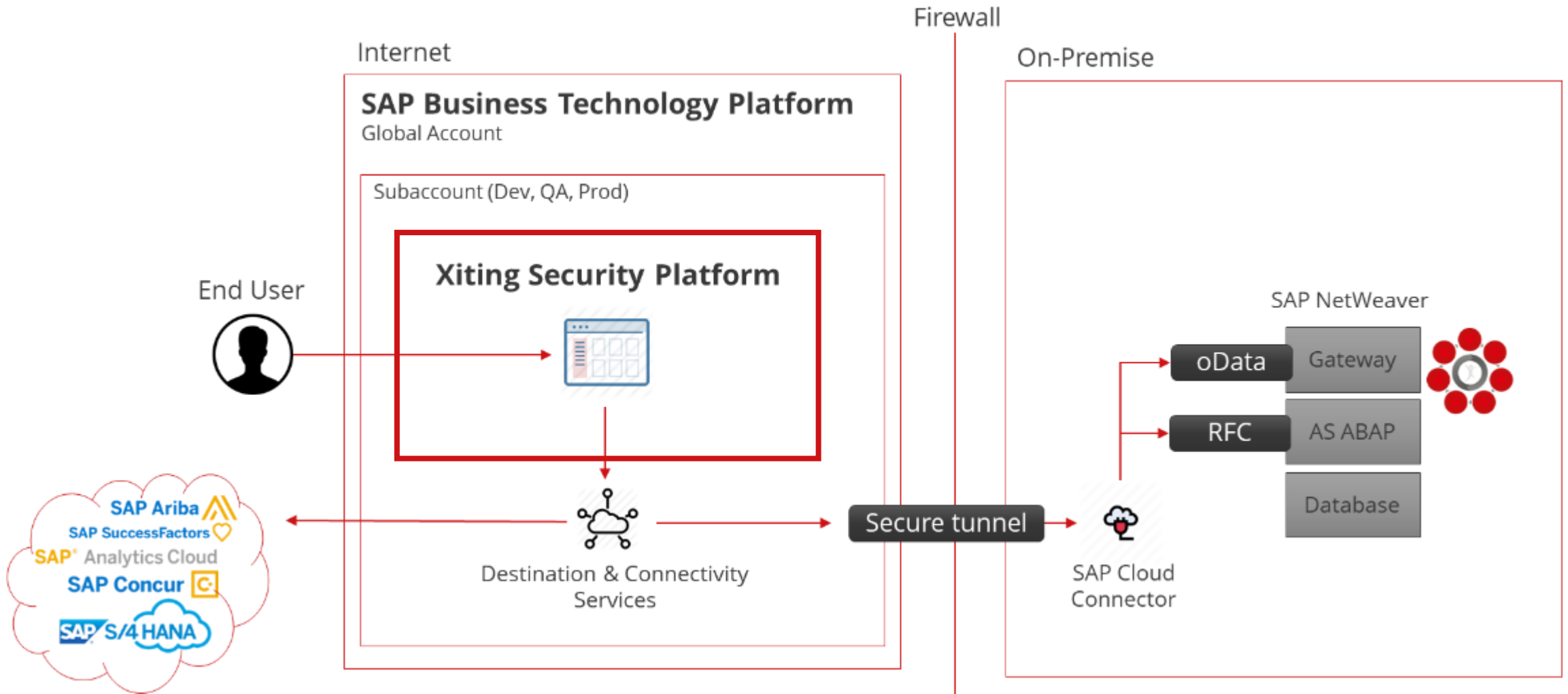
XSMS (XAMS, XCW, XSP)



Die XSP als Single Point of Truth



XSP Architektur

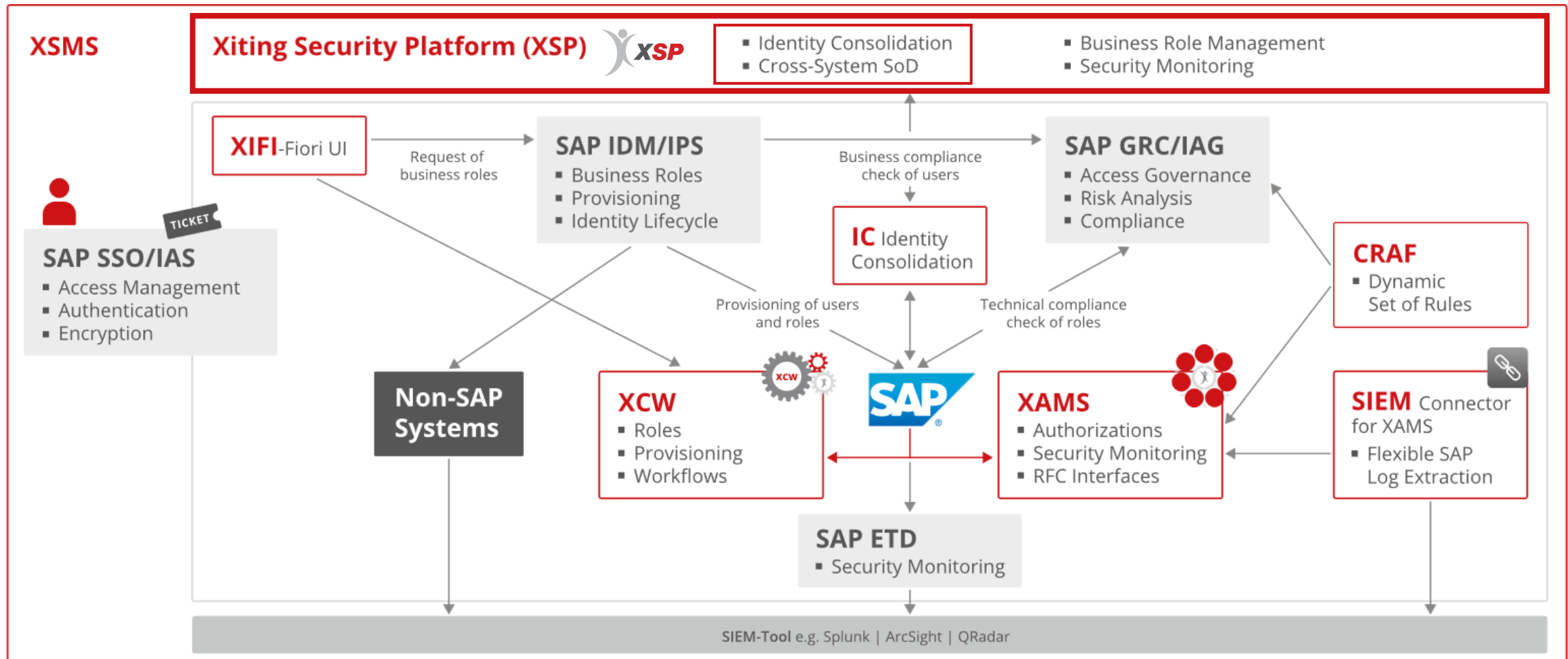


Xiting Security Platform (XSP)

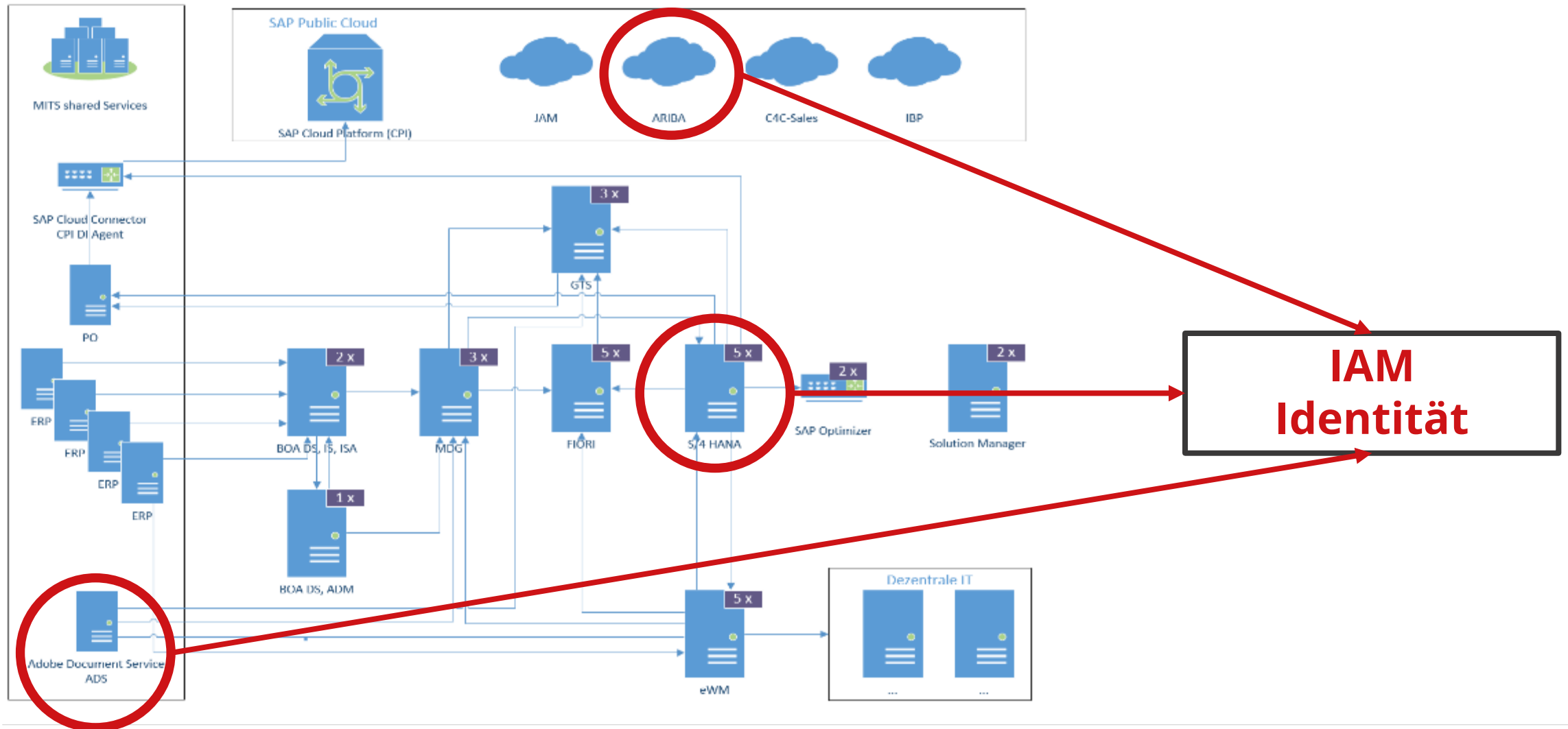
- Zentrale Lösung zur Sicherstellung der Compliance in einer hybriden SAP-Landschaft
- Systemübergreifende Risikoanalysen
- Analyse-Dashboards zur Fehlererkennung und -behebung in der Landschaft
- Zentraler Hub zur Konsolidierung von Identitäten in der hybriden Landschaft
- Security Monitoring und Integration zu SIEM der gesamten Landschaft
- **Erweiterung der vorhandenen Funktionalität der XAMS** und Orchestrierung von Tools und Prozessen
- Die XSP ist das **zentrale Compliance-Cockpit** zur Überwachung der hybriden SAP-Landschaft im Rahmen der **Xiting Security Management Suite**



Die XSP als zentrale cloud-basierte Plattform für die Cloud (und On-Prem)

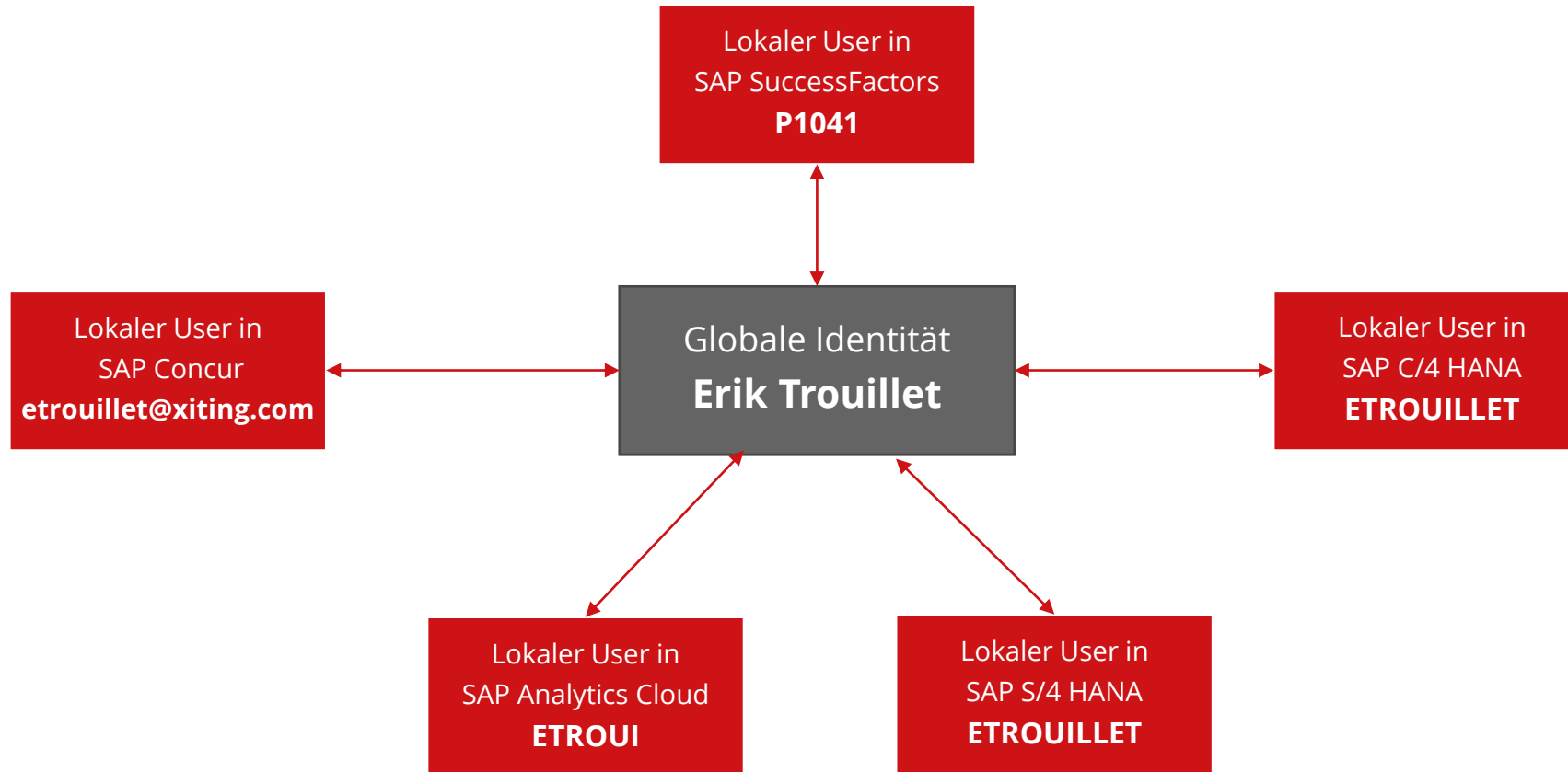


Identitäten in hybriden SAP Landschaften



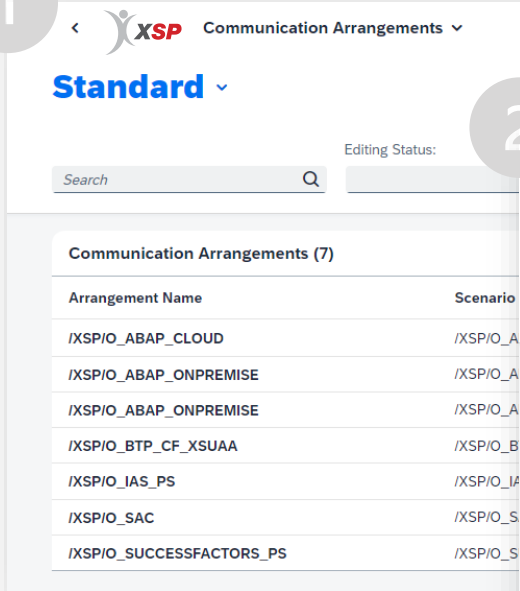
Identity Consolidation

- Konsolidierung der lokalen Benutzer zu einer **globalen Identität**



Schnelle Einrichtung der Identity Consolidation

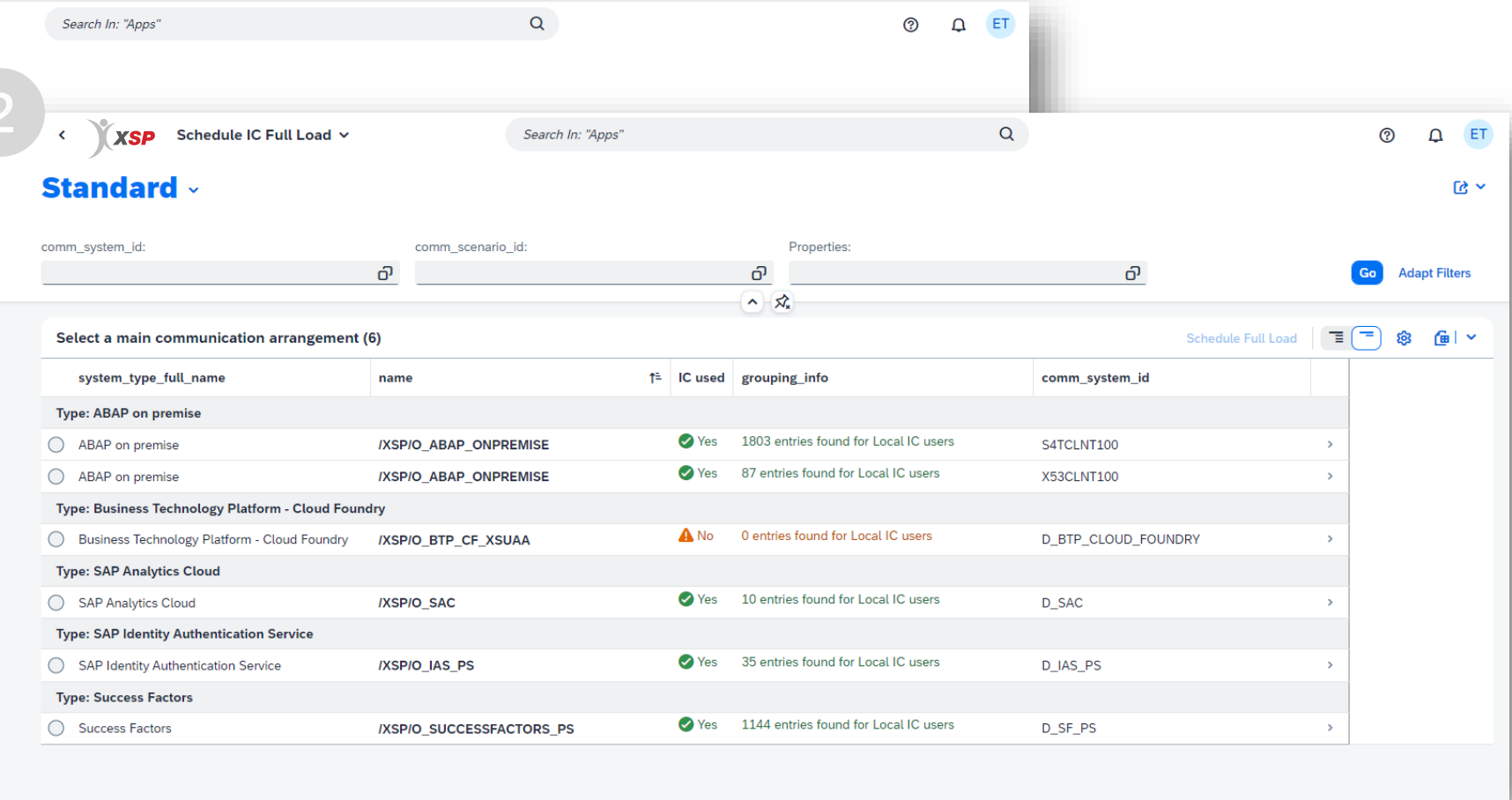
1



Communication Arrangements (7)

Arrangement Name	Scenario
/XSP/O_ABAP_CLOUD	/XSP/O_A
/XSP/O_ABAP_ONPREMISE	/XSP/O_A
/XSP/O_ABAP_ONPREMISE	/XSP/O_A
/XSP/O_BTP_CF_XSUAA	/XSP/O_B
/XSP/O_IAS_PS	/XSP/O_I
/XSP/O_SAC	/XSP/O_S
/XSP/O_SUCCESSFACTORS_PS	/XSP/O_S

2



Schedule IC Full Load

Search In: "Apps"

comm_system_id: [] comm_scenario_id: [] Properties: []

Select a main communication arrangement (6)

system_type_full_name	name	IC used	grouping_info	comm_system_id
Type: ABAP on premise				
<input type="radio"/> ABAP on premise	/XSP/O_ABAP_ONPREMISE	✔ Yes	1803 entries found for Local IC users	S4TCLNT100
<input type="radio"/> ABAP on premise	/XSP/O_ABAP_ONPREMISE	✔ Yes	87 entries found for Local IC users	X53CLNT100
Type: Business Technology Platform - Cloud Foundry				
<input type="radio"/> Business Technology Platform - Cloud Foundry	/XSP/O_BTP_CF_XSUAA	⚠ No	0 entries found for Local IC users	D_BTP_CLOUD_FOUNDRY
Type: SAP Analytics Cloud				
<input type="radio"/> SAP Analytics Cloud	/XSP/O_SAC	✔ Yes	10 entries found for Local IC users	D_SAC
Type: SAP Identity Authentication Service				
<input type="radio"/> SAP Identity Authentication Service	/XSP/O_IAS_PS	✔ Yes	35 entries found for Local IC users	D_IAS_PS
Type: Success Factors				
<input type="radio"/> Success Factors	/XSP/O_SUCCESSFACTORS_PS	✔ Yes	1144 entries found for Local IC users	D_SF_PS



XSP: Eine globale Identität

1

2

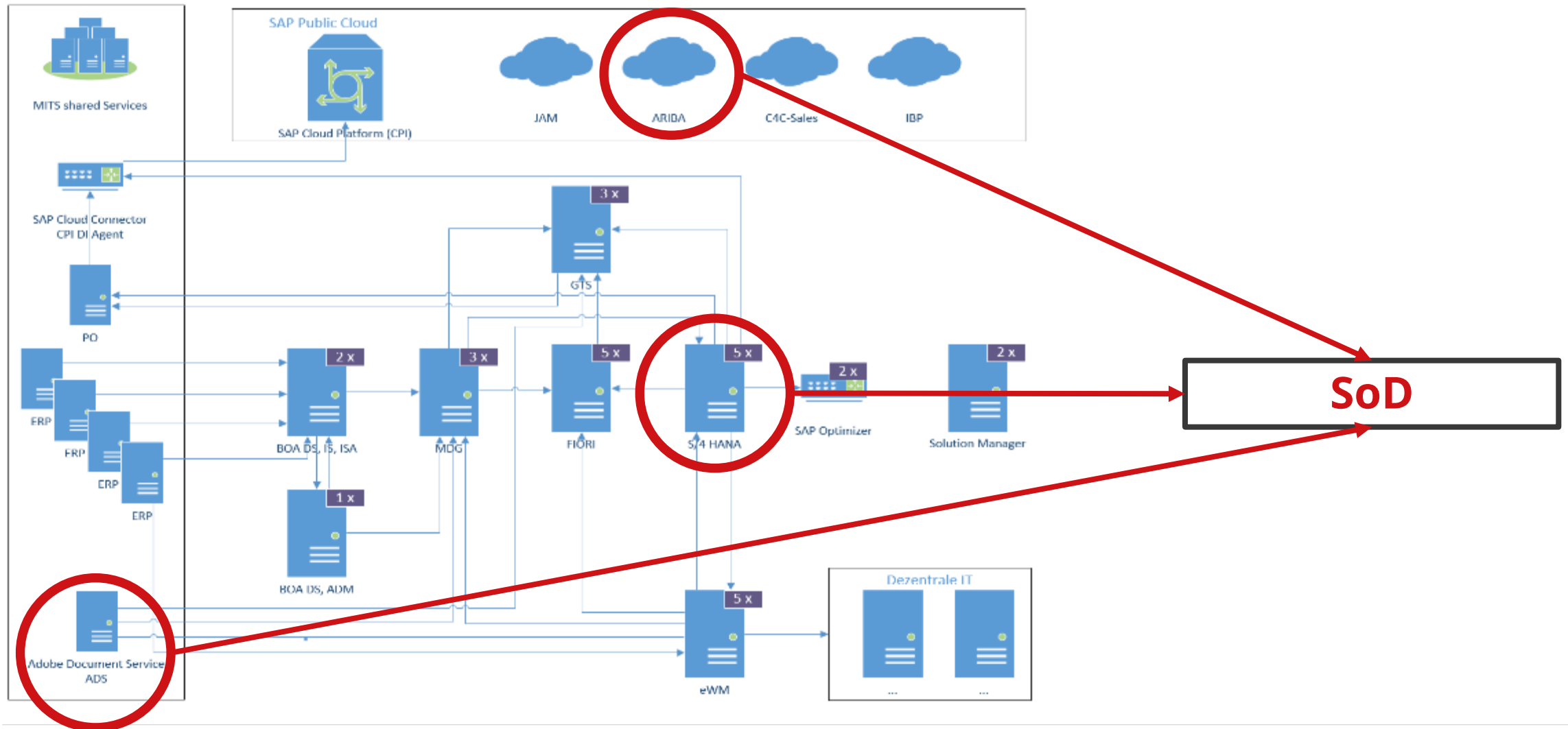
The screenshot shows the SAP XSP IC Global Users interface. It is divided into three main sections:

- Search Section (Step 1):** A search bar at the top with the text "Search In: 'Apps'". Below it, a dropdown menu is set to "Standard". A search filter is applied, showing a table with columns "email", "userid", and "firstname". The results show "etrouillet@xiting.com", "ETROUILLET", and "Erik".
- User Details Section (Step 2):** A detailed view of the user "Erik Trouillet" with email "etrouillet@xiting.com". It includes tabs for "General Information", "Summary", and "Local Users". The "Summary" tab is active, showing statistics: local user - total: 5, local user - invalid: 0, local user - valid: 5, consistency %: 100.00, local user - deleted: 0.
- Local Users Section:** A table listing local users for the selected user.

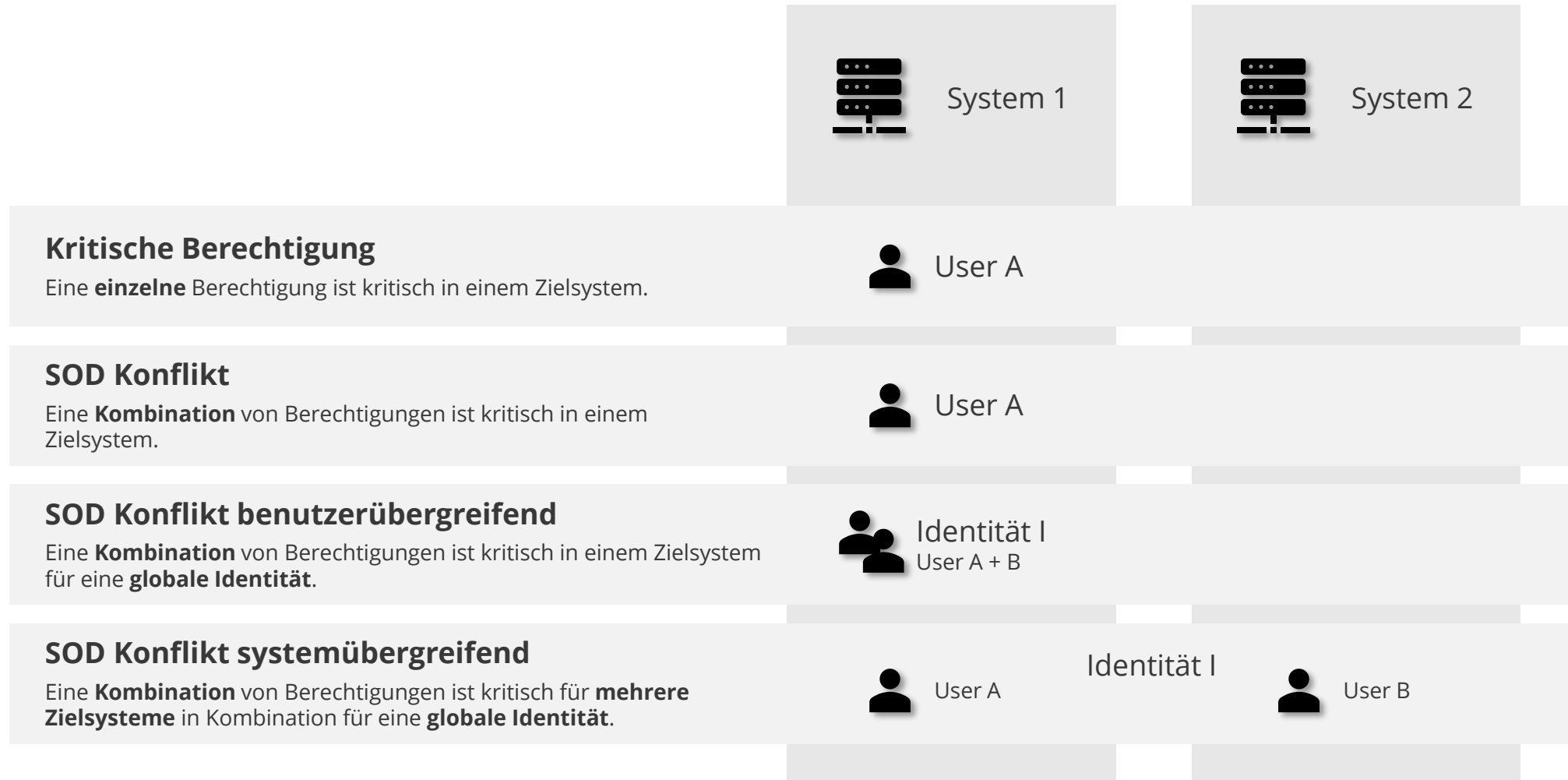
User ID	Short Descript.	comm_system_id	system_type_full_name
ETROUILLET	Valid	S4TCLNT100	ABAP on premise
ETROUILLET_T	Valid	S4TCLNT100	ABAP on premise
T_ADMIN_X	Valid	S4TCLNT100	ABAP on premise
ETROUILLET	Valid	X53CLNT100	ABAP on premise
22b2378a-151c-4608-a778-7a9c062dcb3c	Valid	D_IAS_PS	SAP Identity Authentication Service



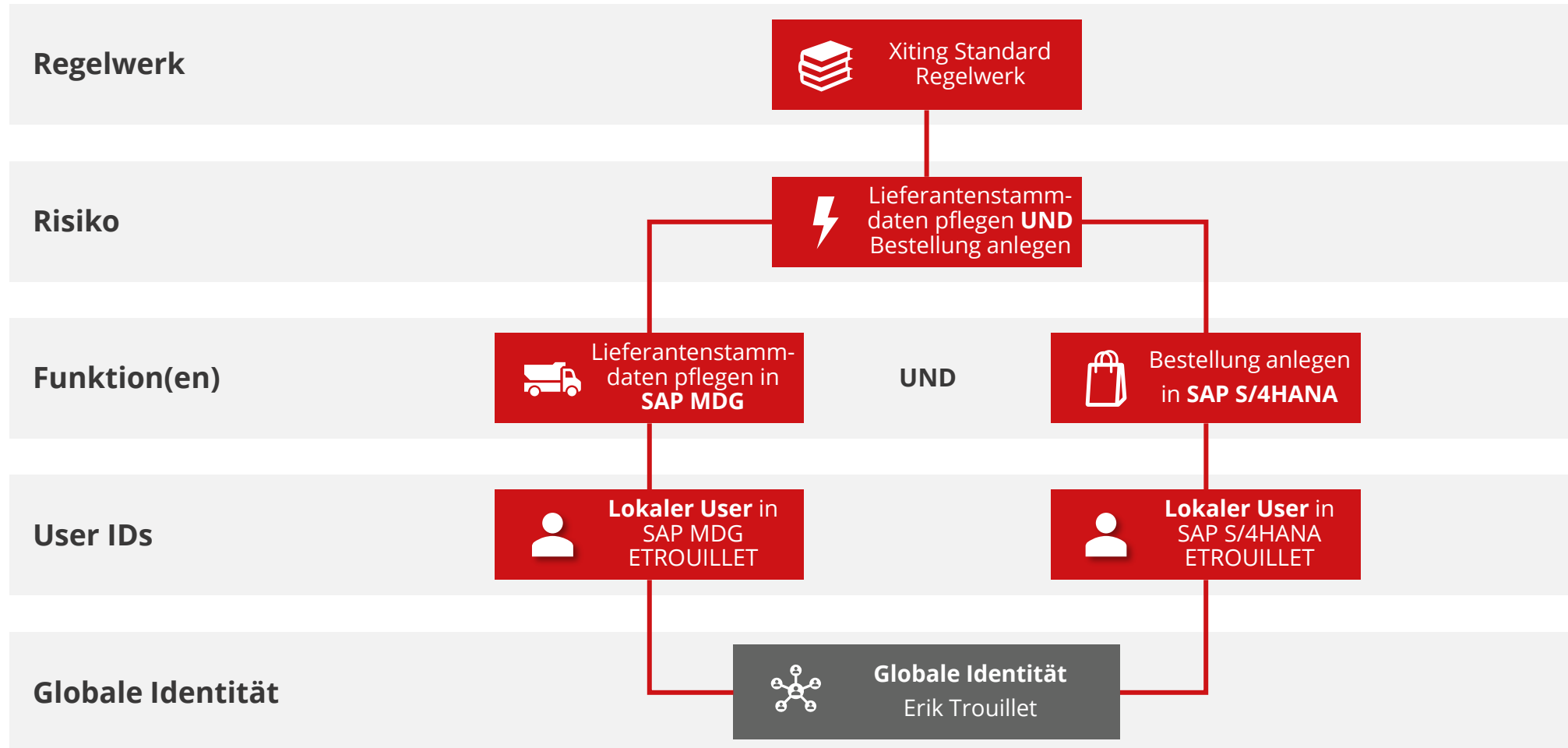
Systemübergreifende Risiken in hybriden SAP Landschaften



Die verschiedenen Risikoarten



Systemübergreifende Risikoanalyse



XSP: Ein zentrales Regelwerk

The image displays three overlapping screenshots of the XSP (SAP Security Group) web interface, illustrating its central role in GRC (Governance, Risk, and Compliance) in the cloud. The screenshots are numbered 1, 2, 3, and 4.

- Screenshot 1:** Shows the 'Standard' Rulesets view. It includes an 'Editing Status' dropdown set to 'All' and a list of 'CRAF Ruleset ID' with checkboxes for 'Xiting'.
- Screenshot 2:** Shows the 'Risks' view for the 'Standard' ruleset. It lists several risk entries with IDs like '/XITING/FI_PER1', '/XITING/FI_FWK1', '/XITING/FIPU5', and '/XITING/FIAP3'.
- Screenshot 3:** Shows the 'Risk' detail view for the risk ID '/XITING/FIPU5'. It displays 'Risk Level: 3' and a 'Description' of 'Combination --> FI: Purchase of data'.
- Screenshot 4:** Shows the 'Function Definition' view for the function ID '/XITING/MM_BES1'. It includes 'System Type ID: ABAP_OP' and a table of function references.

G.	P...	Type	Function Reference	Object	Field	Low
GR01	0	AUTH		M_BEST_BSA	ACTVT	01
GR01	1	AUTH		M_BEST_BSA	ACTVT	02
GR01	2	AUTH		M_BEST_BSA	ACTVT	06
GR02	0	AUTH		M_BEST_EKG	ACTVT	01
GR02	1	AUTH		M_BEST_EKG	ACTVT	02
GR02	2	AUTH		M_BEST_EKG	ACTVT	06
GR03	0	AUTH		M_BEST_WRK	ACTVT	01
GR03	1	AUTH		M_BEST_WRK	ACTVT	02
ABAP_OP	3		ABAP_OP	Purchasing: Create or change purchase orders		
ABAP_OP	4		ABAP_OP	Accounts Payable: Vendor master data maintenance (central)		



Unterstützung von anderen SAP und Non-SAP Lösungen

The screenshot shows the SAP SuccessFactors Functions configuration interface. At the top, there is a navigation bar with a back arrow, the XSP logo, and the text "Success Factors Functions". On the right side of the navigation bar, there are icons for search, help, notifications, and a user profile labeled "ET". Below the navigation bar, there are two tabs: "General Information" (which is active) and "Function Definition".

Under the "General Information" tab, there are three fields:

- Function ID: SF01
- System Type: SF
- Description: User Administration

Below this, there is a section titled "Function Definition". It features a dropdown menu set to "Standard" and a table with the following columns: "G...", "Po...", "Type", "Function Reference", "Permission", and "Operator".

G...	Po...	Type	Function Reference	Permission	Operator
GR00	0	AUTH		ADMINV2_ALLOW_INCLUDE_INACTIVE_USERS	OR
GR01	0	AUTH		ADMINV2_FEATURE_MANAGE_EMPLOYEE_DY NAMIC_GROUPS	OR
GR02	0	AUTH		ADMIN_ACCOUNT_RESET	OR
GR03	0	AUTH		ADMIN_ADD_NEW_USER	OR
GR04	0	AUTH		reset_user_password_user_admin	OR



Benutzer Risikoanalyse

The screenshot displays the XSP User Scan interface. At the top, there is a navigation bar with a back arrow, the XSP logo, and a dropdown menu for 'User Scan'. On the right side of the navigation bar, there are icons for search, help, notifications, and a user profile labeled 'ET'. Below the navigation bar, the main title 'ZTEST' is displayed in large blue letters. To the right of the title, there are several action buttons: 'Edit' (highlighted in blue), 'Delete', 'Start Scan', 'Neuralyzer', and a share icon. Below the title and buttons, there are five tabs: 'General Information' (selected), 'Scan Result', 'Scan Scope', 'User Scope', and 'System Scope'. The 'General Information' tab is active and shows a grid of key-value pairs: 'CRAF Scan Status: FINISHED', 'Description: -', 'Created at: 05/05/2023, 11:10:22', 'Created by: CB9980000010', 'Last changed at: 05/05/2023, 17:59:59', and 'Last changed by: CB9980000010'. Below this, the 'Scan Result' tab is selected and highlighted with a red border. It contains a section titled 'Risk Findings per User' with a dropdown menu showing 'Scan Results (1) | Standard'. Below this is a table with the following data:

Email	Firstname	Lastname	Risk C...
ssg@xiting.com	SSG DE	Test User 1	1 >

Below the table, the 'Scan Scope' tab is selected. It shows a 'General' section with 'Scan Type: RULESET' and a 'Ruleset' section with 'Ruleset: Xiting'.

Resultate adhoc einsehbar sobald die Prüfung abgeschlossen wurde.



User Scope

General

Scan all users for selected systems:
No

Global Users

Standard* ▾



User	Firstname	Lastname	UserId	
ssg@xiting.com	SSG DE	Test User 1	SSG_DE_01	Globale Identität

System Scope

General

Scan all systems for selected users:
No

Communication Arrangements

Standard ▾



Communication Arrangement	System ID	Scenario ID	
/XSP/O_ABAP_ONPREMISE	S4TCLNT100	/XSP/O_ABAP_ONPREMISE	System Scope
/XSP/O_ABAP_ONPREMISE	X53CLNT100	/XSP/O_ABAP_ONPREMISE	



Benutzer Risikoanalyse: Resultate

1

2

< XSP Scan Result
Q ? 🔔 ET

ZTEST /

General Information
Risk Results

Scan

CRAF Scan Name: ZTEST	Scan Type: RULESET
CRAF Scan Status: FINISHED	Description: -

Risk Results

Standard* ▾

CRAF Risk ID	Description
/XITING/FIPU5	Combination -->

< XSP Scan Users
Q ? 🔔 ET

ZTEST / Scan Result /

General Information
Function Results

General Information

Risk		Global User
CRAF Risk ID: /XITING/FIPU5	Criticality: 3	Email: ssg@xiting.com
Description: Combination --> FI: Purchase order & vendor master data	Risk Type: SOD	Lastname: Test User 1
		Firstname: SSG DE
		Userid: SSG_DE_01

Risiko betrifft eine Globale Identität.

Function Results

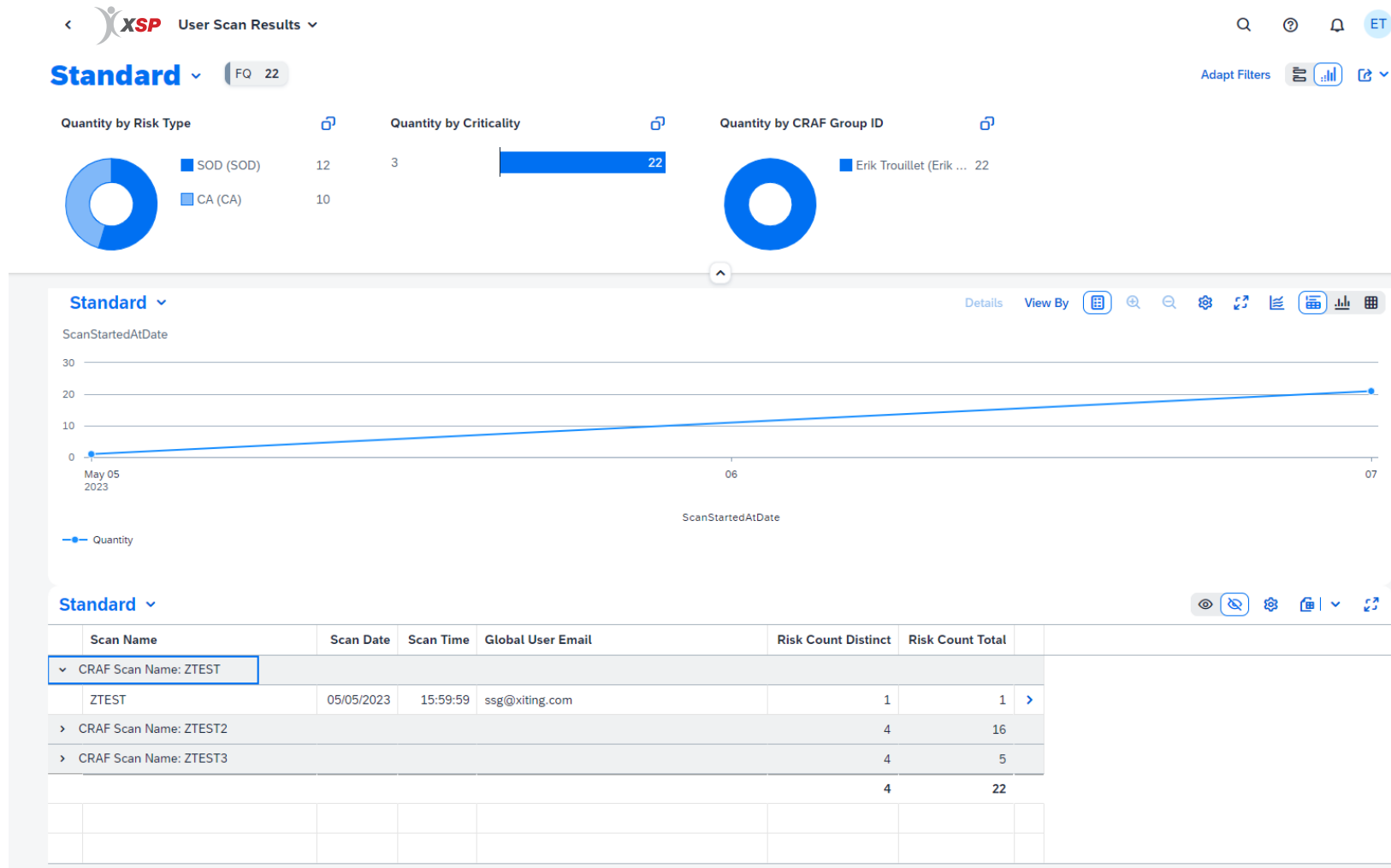
Standard ▾

Function	System Type ID	Description	Userid	Communication Arrangement
/XITING/AP_ACC4	ABAP_OP	Accounts Payable: Vendor master data maintenance (central)	SSG_DE_02	/XSP/O_ABAP_ONPREMISE >
/XITING/MM_BES1	ABAP_OP	Purchasing: Create or change purchase orders	SSG_DE_01	/XSP/O_ABAP_ONPREMISE >

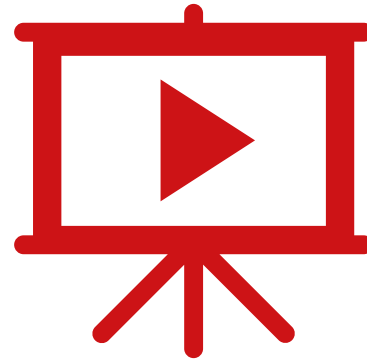
Zwei verschiedene User IDs verursachen den SOD Konflikt.



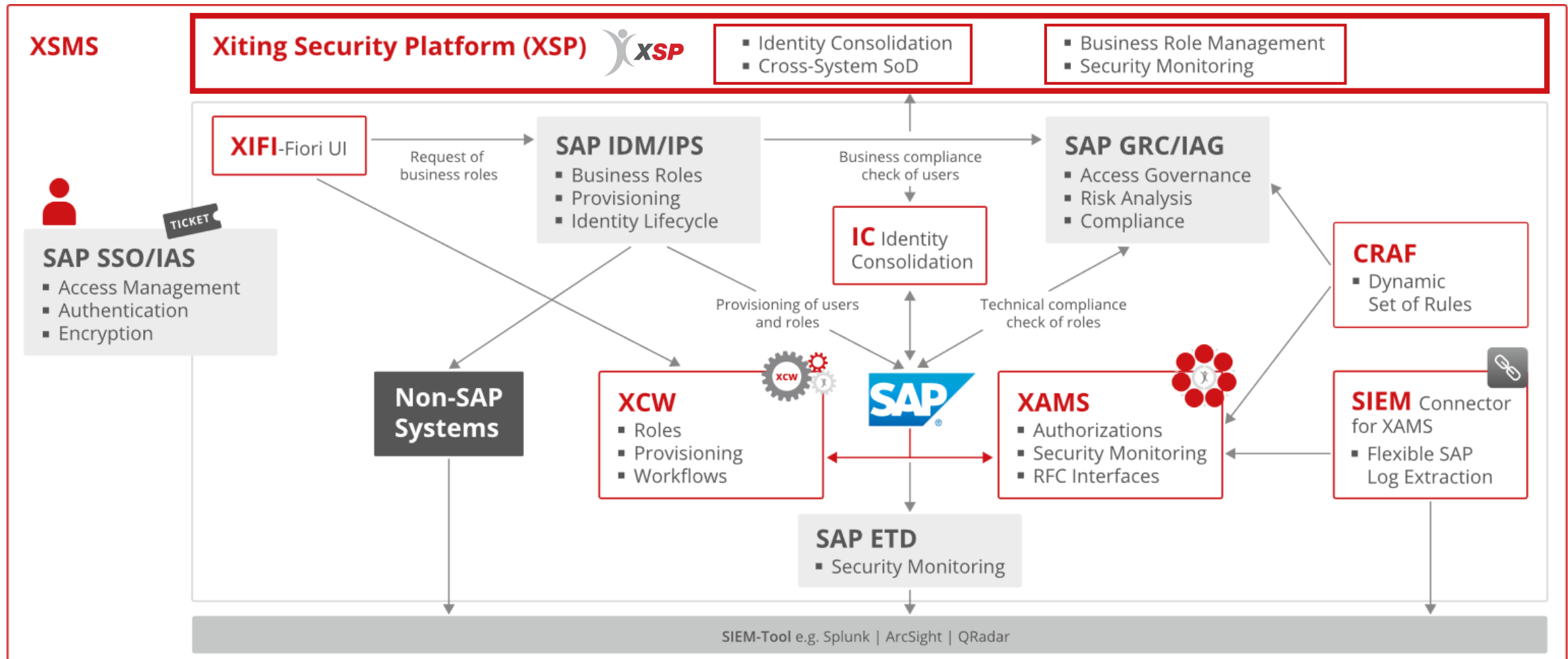
Benutzer Risikoanalyse: Neue Auswertungsmöglichkeiten



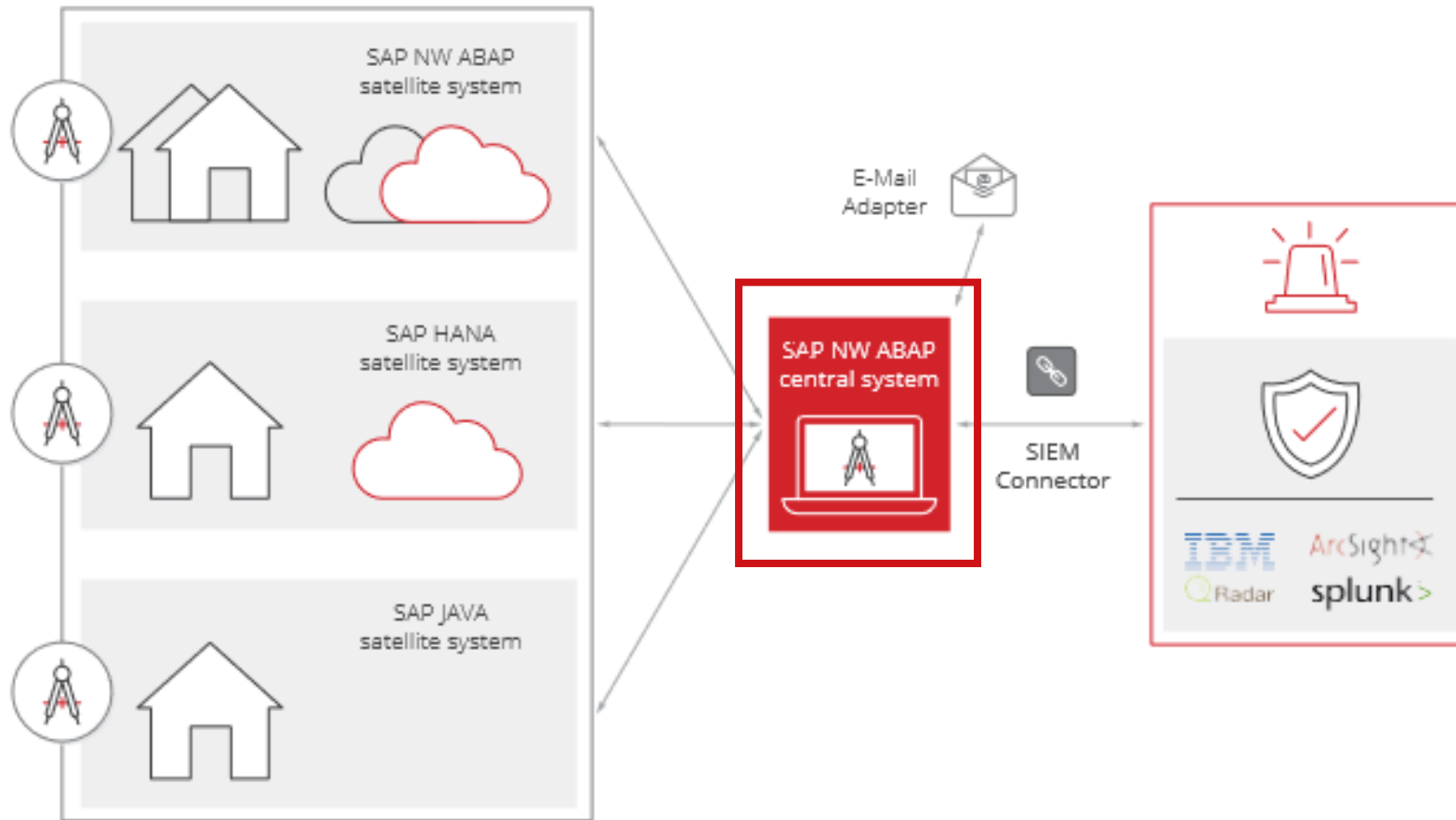
DEMO



Governance, Risk, Compliance und Security aus einer Hand



Bereitstellung der Daten für ABAP Systeme mit dem XAMS Security Architect



Erfüllung der GRC Anforderungen mit der XSP

- Die XSP wird von Grund auf als GRC-Tool entwickelt und soll sämtliche Anforderungen nativ erfüllen. Es werden die Stärken der XAMS genutzt um vor allem in den Bereichen Sicherheit und Skalierbarkeit profitieren zu können.



Governance-
Unterstützung



Risikomanagement



Compliance-
Management



Reporting- und
Analysefähigkeiten



Benutzer-
freundlichkeit



Integration



Sicherheit



Skalierbarkeit



Kapitel 4

Roadmap: Ein Ausblick

XSP Roll-out Plan

01

XSP Framework

Vision, Ziele, Planung
Grobkonzept,
Entscheid Technologie,
Integration, Infrastruktur

02

POC (intern)

Entwicklung Communication
Framework, Identity
Consolidation, Risk Analysis

03

POC (Pilotkunden)

Testphase und
Weiterentwicklung XSP

04

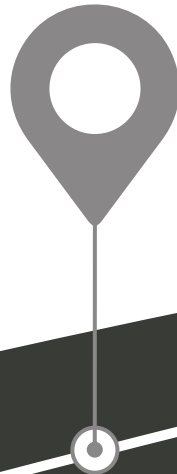
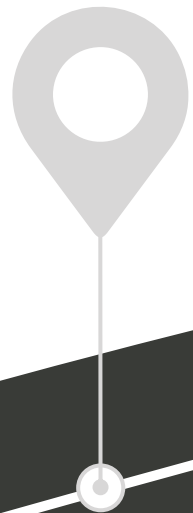
Main Release

Verfügbarkeit der XSP für
Bestands- und Neukunden

05

Feature Packs

Erweiterung der XSP mit
kurzen Releasezyklen



Use Cases in Planung

Identity & Access Governance

- Identity Consolidation
- Systemübergreifende Risiken
- Auswertungen, Bereinigung und Mitigation
- Role Mining und Business Rollen
- Notfallbenutzermanagement
- Security Audits

Security Monitoring & Threat Detection

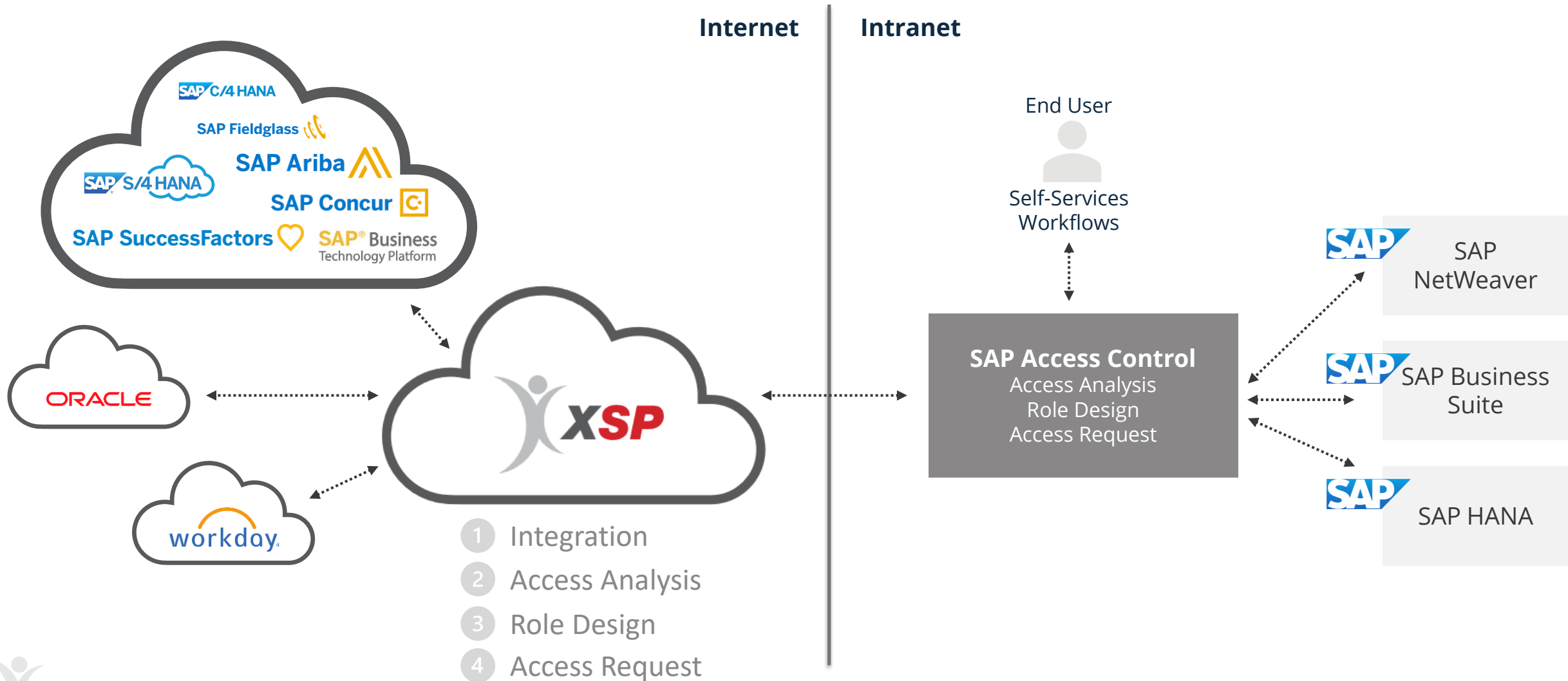
- Zentrales Security Monitoring für sämtliche SAP Applikationen
- Echtzeit Alarmierung
- SIEM Integration
- Erkennung von Bedrohungen und Betrug
- SOAR

Workflows

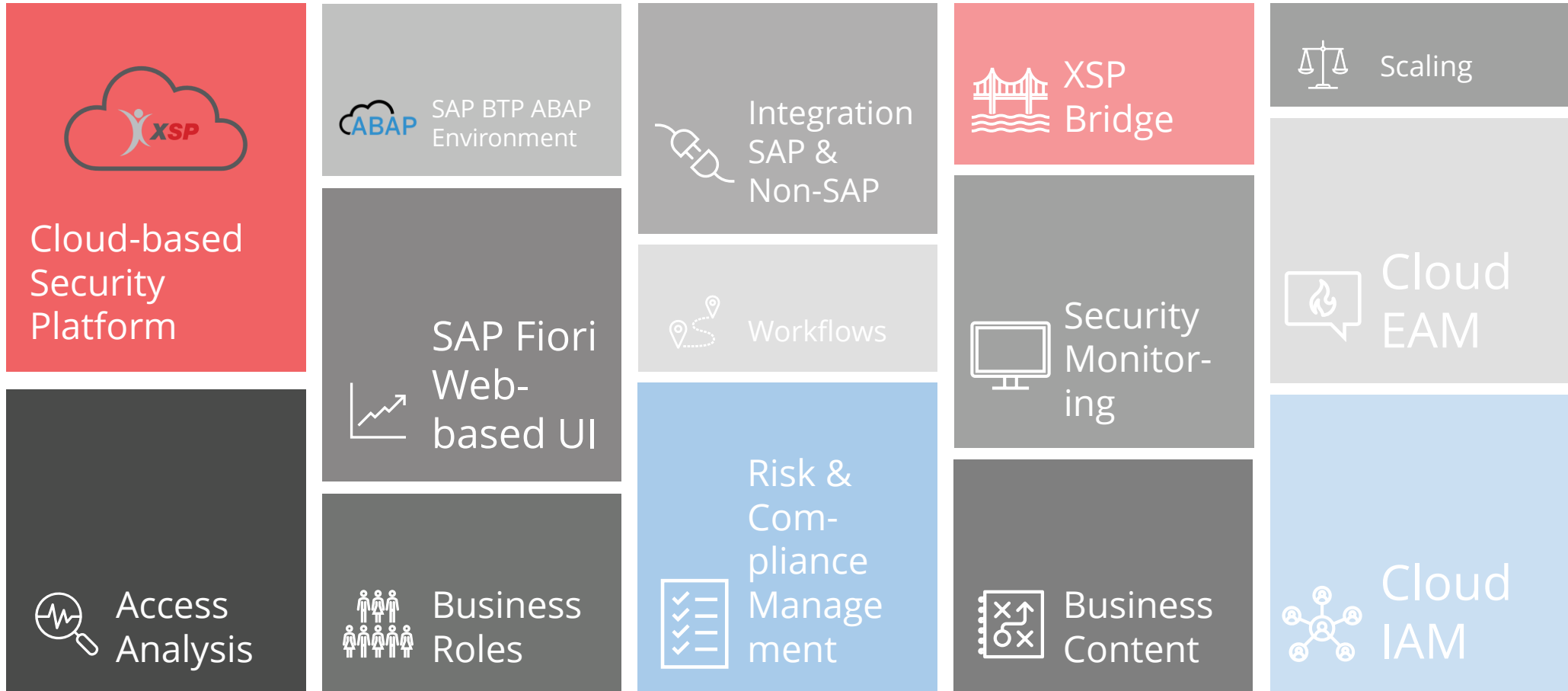
- Regelkonforme Provisionierung von Berechtigungen
- Simulation SOD / Kritische Berechtigungen als Teil von Workflows
- Benutzer-Rezertifizierung



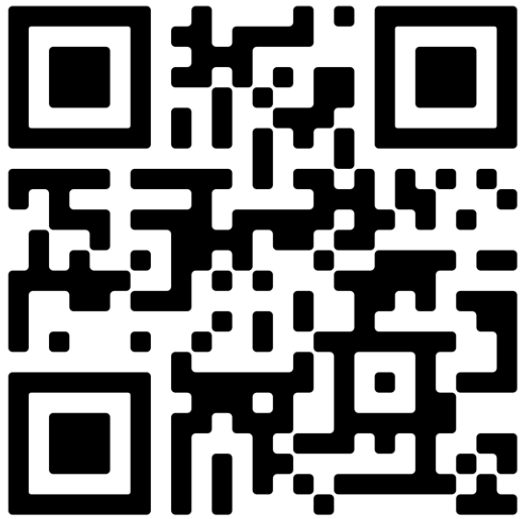
XSP Bridge



XSP im Überblick



Xiting Security Platform – Schauen Sie mal vorbei

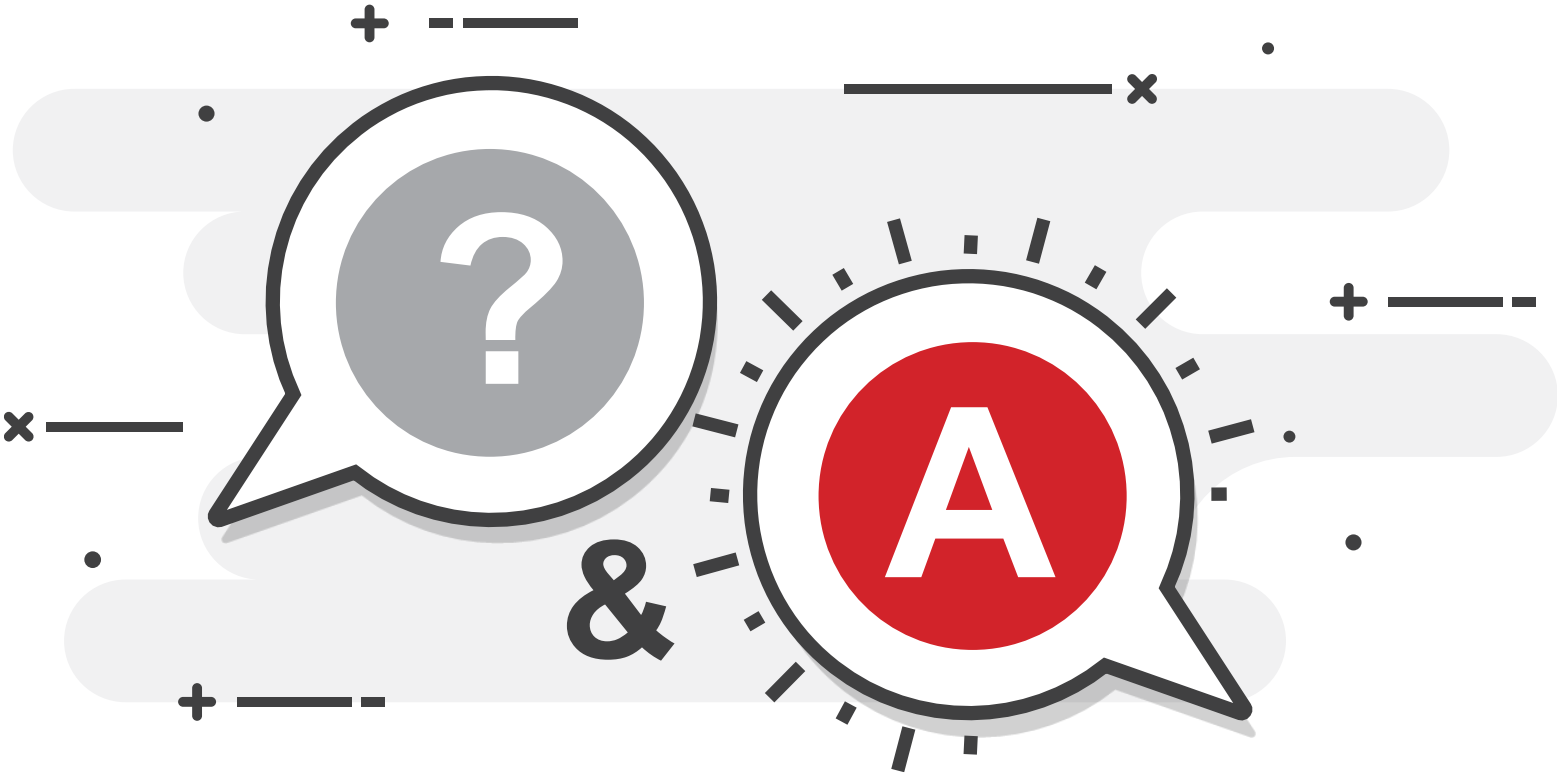


SCAN ME

Revolutionieren Sie Ihr
SAP Security Management
mit der
Xiting Security Platform (XSP)



Fragen und Diskussionen



Fragen und Diskussionen



Erik Trouillet

Managing SAP
Security Consultant



Olaf Sauer

Leiter Direct Sales

Dankeschön

Für Ihre Aufmerksamkeit

Wenn Sie weitere Informationen benötigen,
können Sie uns gern kontaktieren.

© 2023 Xiting. All rights reserved.

Alle erwähnten Produkt- und Dienstleistungsamen sind Marken der jeweiligen Unternehmen.
Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung der Xiting AG in
irgendeiner Form oder zu irgendeinem Zweck vervielfältigt oder übertragen werden.
Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

