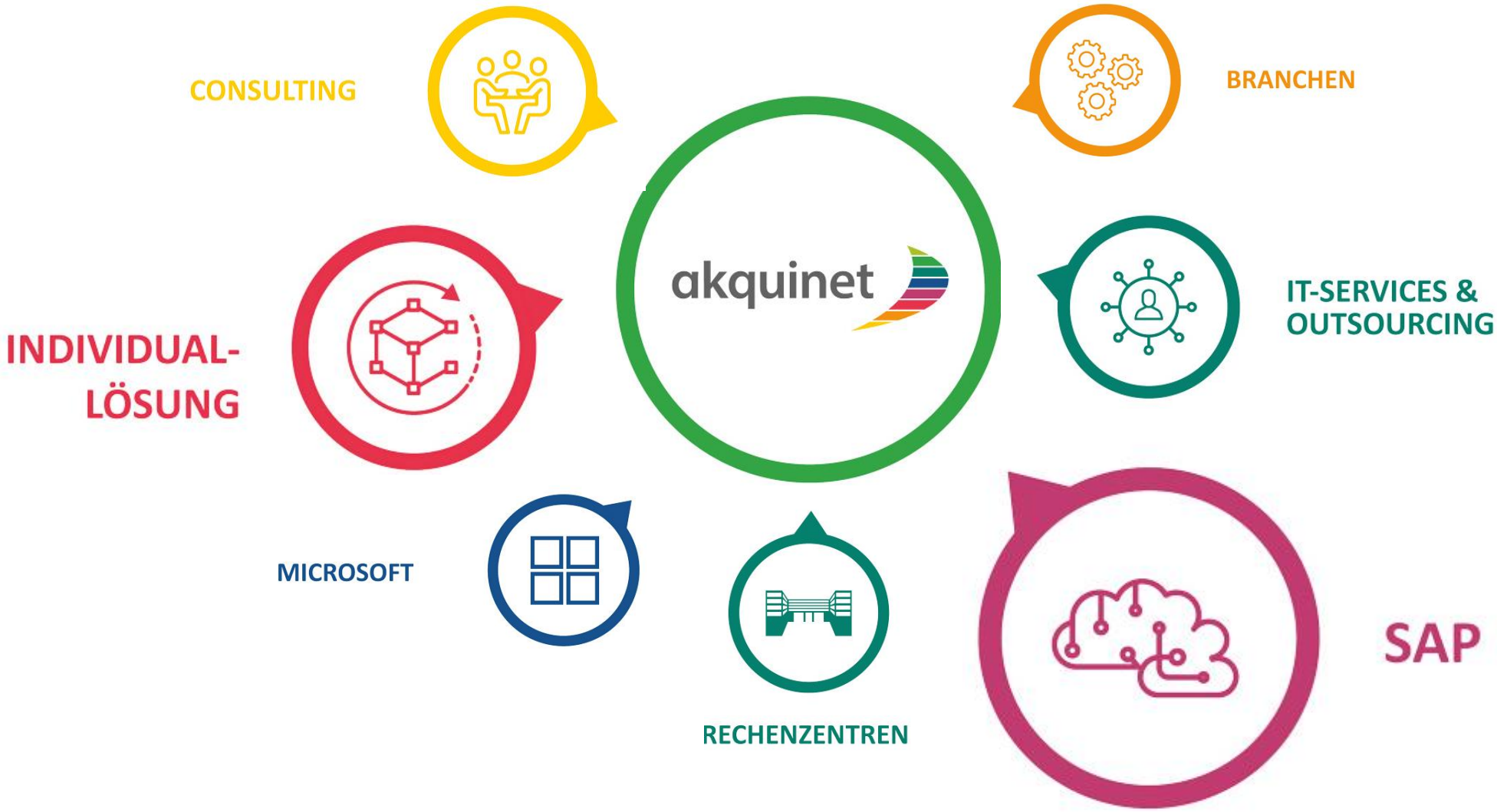
akquinet

SAP Security & Compliance: Get Clean & Stay Clean

Am Beispiel eines Industrieunternehmens

AKQUINET-Leistungsumfang



Ganzheitliche SAP Security & Compliance

Das sollte das Ziel sein:

1. Erfassung und Bewertung aller wesentlichen Risiken.
2. Regelmäßige und systematische Informationserhebung.
3. Zeitnahe und zuverlässige Informationsweiterleitung.
4. Ganzheitliche Betrachtung der Risikosituation in Ihrem Unternehmen.
5. Behandlung von Risiken unter der Prämisse der Wirtschaftlichkeit.
6. Kultur der Akzeptanz und offenen Kommunikation von Risiken in Ihrem Unternehmen.

Schaffung eines Instrumentariums, das die zeitnahe Steuerung aller wesentlichen operativen und strategischen Risiken ermöglicht.

SAP-Security mit AKQUINET: Unsere GRC-Suite.

Absicherung von über
2.000
SAP-Systemen weltweit

Über
1,5 Millionen
SAP-Benutzer

Rund
200 Kunden
vertrauen auf uns

SAST

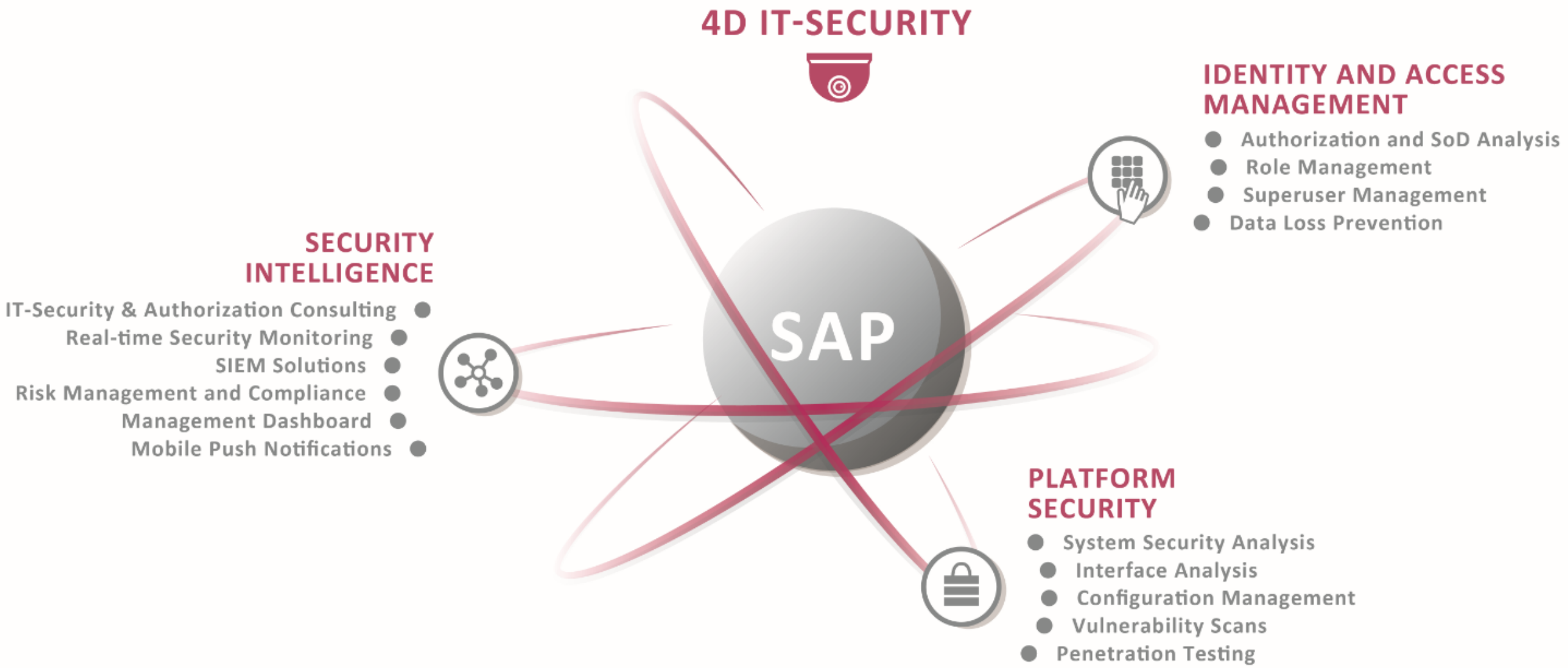
Mehr als
4.000
automatisierte System-Checks
und aktuelle Security Notes

3-fach
SAP-zertifiziert und
geprüft von Big4-WPG

Vordefinierte
25 Prüfregelwerke
gegen SoD-Konflikte

Rundumschutz für Ihre SAP-Systeme in Echtzeit!

Mit der AKQUINET GRC-Suite „SAST“



Referenzen aus dem Bereich SAP-Security

akquinet

Kunststoffe

ALBIS

Produktion

amag

Chemie

BÆRLOCHER

Konsumgüter

BRITA

Nahrungs- und Genussmittel

CSM

Dienstleistung ITK

DEMANDO

Grundstücks- und Wohnungsbau

Deutsche Wohnen

Maschinenbau

ENGEL

Dienstleistung ITK

finanz informatik technologie service

Baugewerbe

HEIDELBERGCEMENT

Energieversorgung

kelag

Chemie / Textilindustrie

LENZING

Wasserwirtschaft

Berliner Wasserbetriebe

Automobilzulieferer

MAGNA

Technologie / Chemie

THE LINDE GROUP

Konsumgüter

Miele

Produktion / Dienstleistung

Minol

Konsumgüter

MONT BLANC

Handel

PUMA

Maschinenbau

PALFINGER

Versicherungen

R+V

Handel

s.Oliver

Banken / Versicherungen

Sparkassen Versicherung

Pharmazeutik

Takeda

Gesundheitswesen

UKE HAMBURG

Banken

Union Investment

Grundstücks- und Wohnungsbau

VIVAWEST

Maschinen- und Anlagenbau

WFL MILLTURN TECHNOLOGIES

Bergbau

wolfram

BWB und SAST: Überblick wesentlicher Themen 2014-2022

2014: Ausschreibung „GRC-Tool“ >> SAST Suite

- Vorbereitung auf den Wirtschaftsprüfer (IT-Audit)
- Analysen im Bereich Benutzer / Rollen, Berechtigungsprozesse und Schnittstellen
  - Funktionstrennungskonflikte (Segregation of Duties – SoD)
  - Kritische Berechtigungen (Sensitive Transactions – ST)
- Berechtigungs-Teilprojekte, z.B. Konzeption / Rollenbau / Rollout bzw. Anpassungen
- UAM-Web Antragsformular (vs. manueller „Papier“-Antrag) im Kontext Identity & Access Management / Einführung Password Reset
- 360 Grad Echtzeitüberwachung inkl. Download Management (Schutz vor unbeabsichtigtem Verlust / Datenabfluss)
- Notfallbenutzer-Prozessdesign und Implementierung
- Analysen Benutzer / Gültigkeitszuordnung / Entwicklerschlüssel und Lizenzauswertung
- Auswertungen und Ergebnisbereitstellung im Kontext Systemische Sicherheitsanalyse (SSV)

„Auch die Wirtschaftsprüfer stellen fest, dass sich die SAP Security und Compliance stetig verbessert“

akquinet

GET CLEAN

Herstellung des sicheren Betriebs-zustands

Pragmatismus des Alltags an einem Beispiel:

1. Mitarbeiter Thorsten ist Logistiker.
2. Er wechselt von der Disposition in den Einkauf.
   Die ersten 3-6 Monate soll er aber noch in seiner alten Tätigkeit unterstützen.
3. Thorsten beginnt im Einkaufsteam für die Warengruppe für die DIN- und Normteile.
4. Dann wird er in das Team für Investitionsgüter und Werkzeugmaschinen befördert, wo mit gänzlich anderen Wertgrenzen hantiert wird.
5. Hier wird er eingearbeitet, während er parallel seine bisherigen Aufgaben erledigt.

? Könnte es sein, dass er nach 2 Jahren noch Berechtigungen der Logistik hat und noch immer Zugriffe im DIN- und Normteile-Bereich möglich sind?

SAST Authorization Management:
Governance, Riks & Compliance-Konformität für Ihre SAP-Systeme.

Die Herausforderung

- Weitreichende Berechtigungen im SAP begünstigen Fehler und dolose Handlungen.
- Funktionstrennungskonflikte (SoD) verstoßen gegen Compliance-Regeln und stellen ein hohes Sicherheitsrisiko dar.
- Systemübergreifende Analyse und Härtung von Rollen ist zeitaufwändig.
- Erkennung und Behebung von SoD-Konflikten mit Standardmitteln ist quasi unmöglich.
- Erfahrene Berechtigungsspezialisten sind schwer zu finden und dazu kostenintensiv.

Komplexe Berechtigungen stellen oft ein hohes Sicherheits- und Compliance-Risiko dar.

Mit der SAST SUITE können Sie Ihre SAP-Berechtigungen, Kombinationen, Prozesse und SoD-Regelwerke überwachen und auswerten.

SAST Authorization Management:
Governance, Riks & Compliance-Konformität für Ihre SAP-Systeme.

Die Herausforderung

- Eine regelmäßige Optimierung der SAP-Berechtigungen ist für jedes Unternehmen obligatorisch.
- Defizit an Informationen, welche Berechtigungen der Fachbereich tatsächlich benötigt.
- Zu großzügig vergebene Rollen führen zu:
  - erhöhtem Potenzial für Funktionstrennungskonflikte (SoD).
  - Intransparenz durch die Vielzahl der Berechtigungen pro User.
  - unnötigen Kosten im Bereich der SAP-Lizenzen.

Fehlende Analyse über die tatsächliche Nutzung von Transaktionen durch die User.

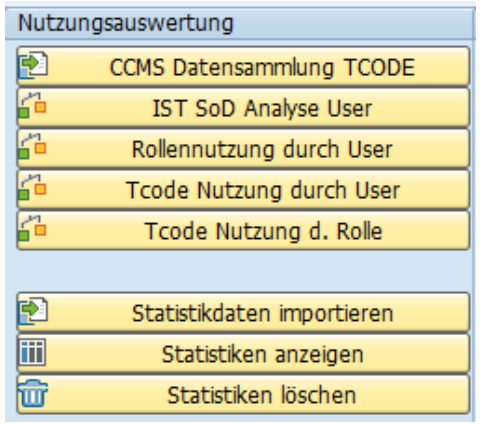
Die SAST SUITE liefert Transparenz und ermöglicht eine reibungslose Umsetzung.

IST-Nutzungsanalyse und IST-SoD-Analyse

Auswertung der IST-Nutzung erlaubt präzise Rückschlüsse über tatsächlich verwendete Anwendungen. Transaktionen, die…

- …ein User nie verwendet, können entzogen werden.
- …kein einziger User verwendet, können aus den Rollen ausgebaut werden.

Auswertungen basieren auf den ST03N Statistiksätzen von SAP und werden monatlich fortgeschrieben.



SAST: Transaktionsnutzung je Benutzer/Rolle

Mandant	Gruppe	Benutzer	Rolle	Bezeichnung der Rolle	Anzahl Tcode	Anzahl benutzt	Prozent
100	FI	RKEMPF	/SAST/ADMINISTRATOR	SAST Administrator	224	168	075 %
100	FI	RKEMPF	/SAST/AUDITOR	SAST Auditor	6	6	100 %
100	FI	RKEMPF	/SAST/ROLE_OPTIMIZER_ADMIN	SAST RoleOptimizer	58	34	059 %
100	FI	RKEMPF	/SAST/USER	SAST User (Aktivierung NotfallID)	4	4	100 %
100	FI	RKEMPF	ZE>EW_EWFF_CS_ADMIN	Customer-Interaction-Center Administration	13	0	
100	FI	RKEMPF	Z_AR_F110	Ausführung des Zahllaufs mit TC F110	91	2	002 %
100	FI	RKEMPF	Z_NUR_SU53	SU53	2	2	100 %
100	FI	RKEMPF	Z_RFC_ACL	S_RFCACL	0	0	
100	FI	RKEMPF	Z_S_RFC_ACL	Z_S_RFC_ACL	0	0	

„Innerhalb eines Quartals lassen sich bis zu 75% der aktuellen Berechtigungen reduzieren.“

Bei unseren Berechtigungsprojekten treffen wir
nicht selten auf User mit 200-500 Berechtigungen.
Benötigt werden davon nur 25% – und wir wissen welche!

Ralf Kempf
CTO SAST SOLUTIONS

Ihre Schritte zu einem erfolgreichen Berechtigungs-Redesign.

Mit dem SAST Safe Go-Live Management gelingt Ihnen das sicher.

- **Testüberwachung**
  - Intuitive Projektverwaltung. Online Überwachung der Nutzung und Aktivitäten aller Test-User.
  - Hohe Transparenz für Testabdeckung und eventuelle Berechtigungsfehler.
- **Fallback-User als Ihr doppelter Boden**
  - Speicherung aller Berechtigungen der User zum Zeitpunkt des Go-Live.
  - Auf Knopfdruck werden alte Berechtigungen im Fehlerfall sofort und ohne Zeitverzug wieder zugewiesen.
  - Erleichterte Vergabe fehlender Berechtigungen

⊕ Stark reduzierter Testaufwand

⊕ Keine Einschränkungen im Tagesgeschäft

⊕ Keine zusätzlichen Lizenzkosten für Referenz-/Fallback-Benutzer

Die Herausforderung

- Hohe Anzahl an Schnittstellen in komplexen Systemlandschaften.
- Schnittstellen sind häufig kaum bis gar nicht dokumentiert.
- Unkontrollierter Datenaustausch.
  - Sicherheitsprobleme
  - Compliance-Verstöße
- Zu großzügige Berechtigungen technischer Nutzer.

Es fehlt an einer vollständigen Übersicht aller Schnittstellen aller SAP-Systeme.

Die SAST SUITE bietet eine umfängliche Übersicht und Absicherung der SAP-Schnittstellen!

Sicherheitsrisiko Systemschnittstellen

Fokus der Absicherung von SAP-Systemen liegt meist auf Berechtigungen von Dialogbenutzern.

Technische Benutzer (RFC und Batch) werden mit weitreichenden Rechten ausgestattet.

Keine aktuelle Dokumentation aller Schnittstellen

Vertrauensbeziehungen zwischen Systemen (SSO und Trusted RFC) sind selten dokumentiert.

Remote Datenbankverbindungen führen zu unkontrollierten Sicherheitslücken.

Der SAP Standard bietet keine umfassende und zentrale Auswertung aller Schnittstellen.

STAY CLEAN

Erhaltung des sicheren Betriebs-zustands

SAST Authorization Management

Proaktive Prüfung auf Funktionstrennungs-Konflikte.

Anfrage nach neuer User-ID und Autorisierung

✓

Genehmigung durch Supervisor

✓

User-Admin weist Rollen zu

User-Admin-Benachrichtigung: ok / nicht ok

SAST Authorization Management

Anwendungszenarien

Reaktive Anwendung

- Ex-post Prüfung von Benutzerstammsätzen und Rollen

Proaktive Anwendung

- Kontinuierliche Identifizierung und Beseitigung von Risiken
- Integration in SAP
  mit dem Profilgenerator (PFCG),
  der Benutzerpflege (SU01, etc.)
  und dem SAST User Access Management
- Simulation von Berechtigungsänderungen

SAST Risk & Compliance Management:
Aktives Risikomanagement für Ihre SAP-Systeme.

akquinet

Die Herausforderung

- Sicherheits- und Compliance-Prüfungen sind kosten- und ressourcenintensiv.
- Risiken müssen umfassend erkannt und mitigiert werden.
- Komplexer Prüfumfang je System mit individuellen Richtlinien.
- Prüfberichte müssen dokumentiert und für verschiedene Zielgruppen aufbereitet werden.
- Es fehlt oftmals an einer Automatisierung für wiederkehrende Aufgaben.

Komplexe Systemlandschaften machen eine Übersicht über alle Risiken fast unmöglich.

Mit der SAST SUITE dokumentieren und mitigieren Sie alle Risiken effektiv und effizient.

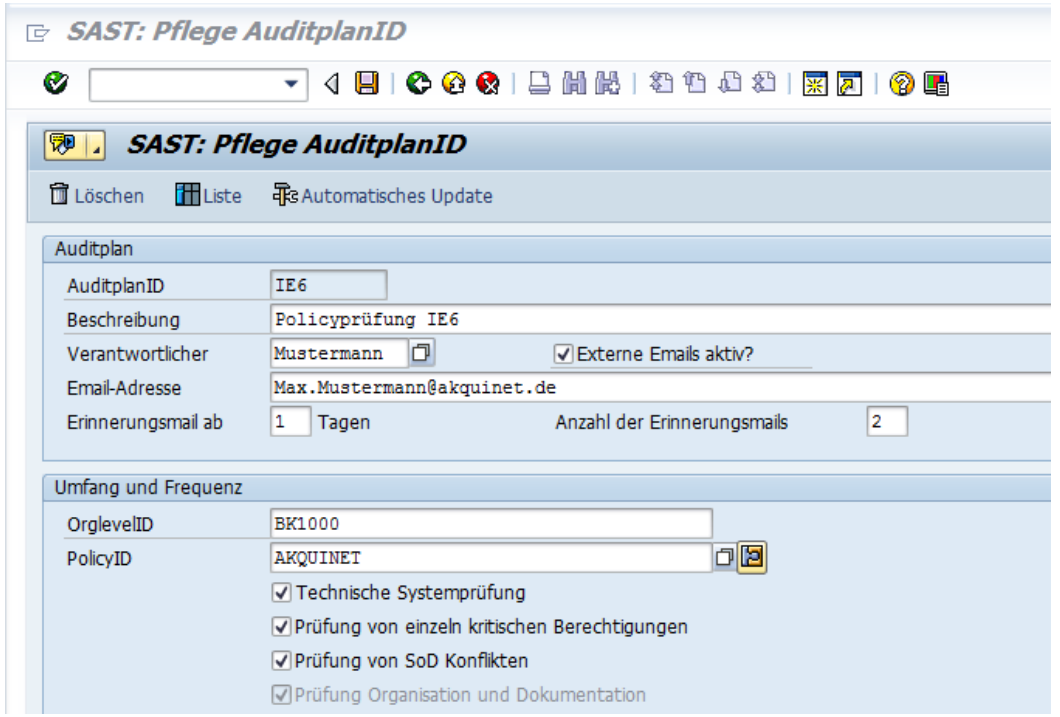
Zyklische Prüfungen mit dem SAST Risk and Compliance Management

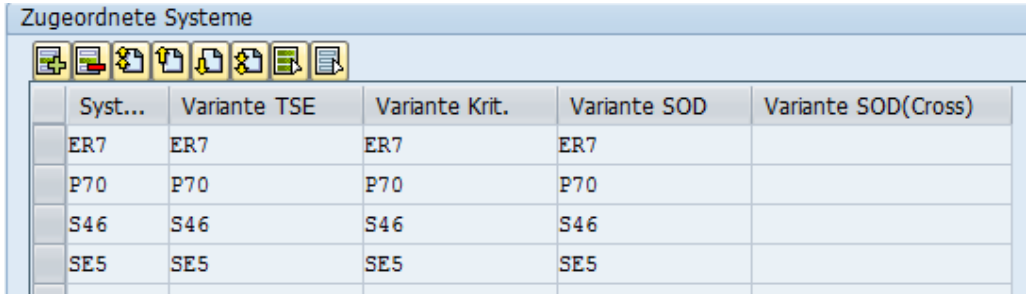
Auditplan

- Definition des Audit-Umfangs
- Planung wiederkehrender Prüfungen
- Automatisierte Audit-Durchführung

ZIEL

Zyklische Prüfung mit gleichem Umfang für das Berichtswesen.





SAST User Access Management:
Governance, Riks & Compliance-Konformität für Ihre SAP-Systeme.

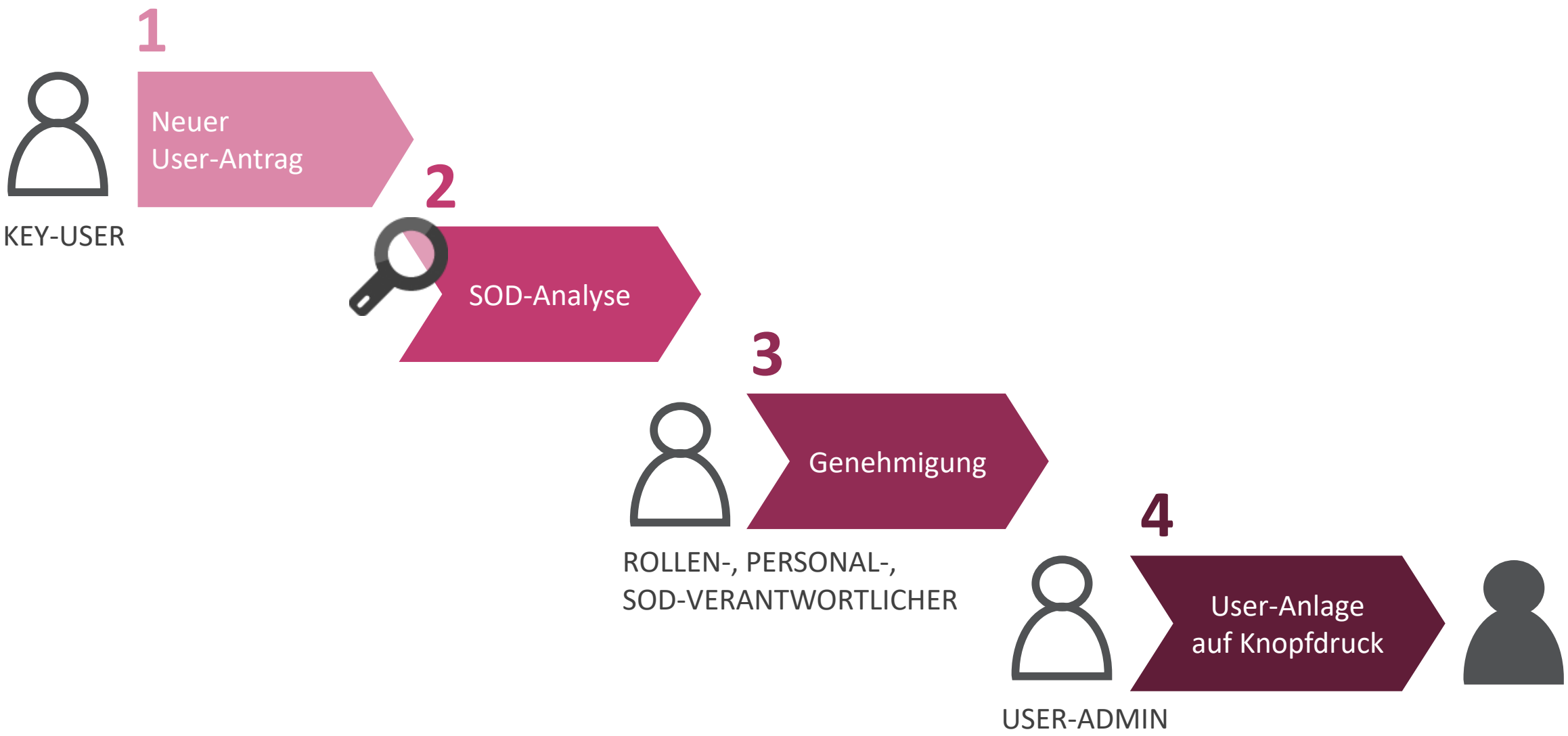
Die Herausforderung

- User-Identitäten und -Berechtigungen können nicht systemübergreifend gepflegt werden.
- Komplexe Rollen- und Berechtigungskonzepte führen zu Unübersichtlichkeit
  - Entstehung von SoD-Konflikten
  - Bereinigung von Rollen wird erschwert
- Aufwand für das Berechtigungsmanagement ist üblicherweise hoch.
- Integration in externe IDM-Systeme nur langwierig und kostenintensiv umsetzbar.

Rollen- und Berechtigungs-Projekte zählen zu den aufwändigsten und teuersten im SAP-Umfeld.

Die SAST SUITE ermöglicht eine effiziente Verwaltung von Rollen und Berechtigungen sowie die Integrationsmöglichkeit von IDM-Systemen.

User Access Management mit der SAST SUITE: Workflow eines User-Antrags



SAST Security Radar:
Echtzeitüberwachung Ihrer SAP-Systeme.

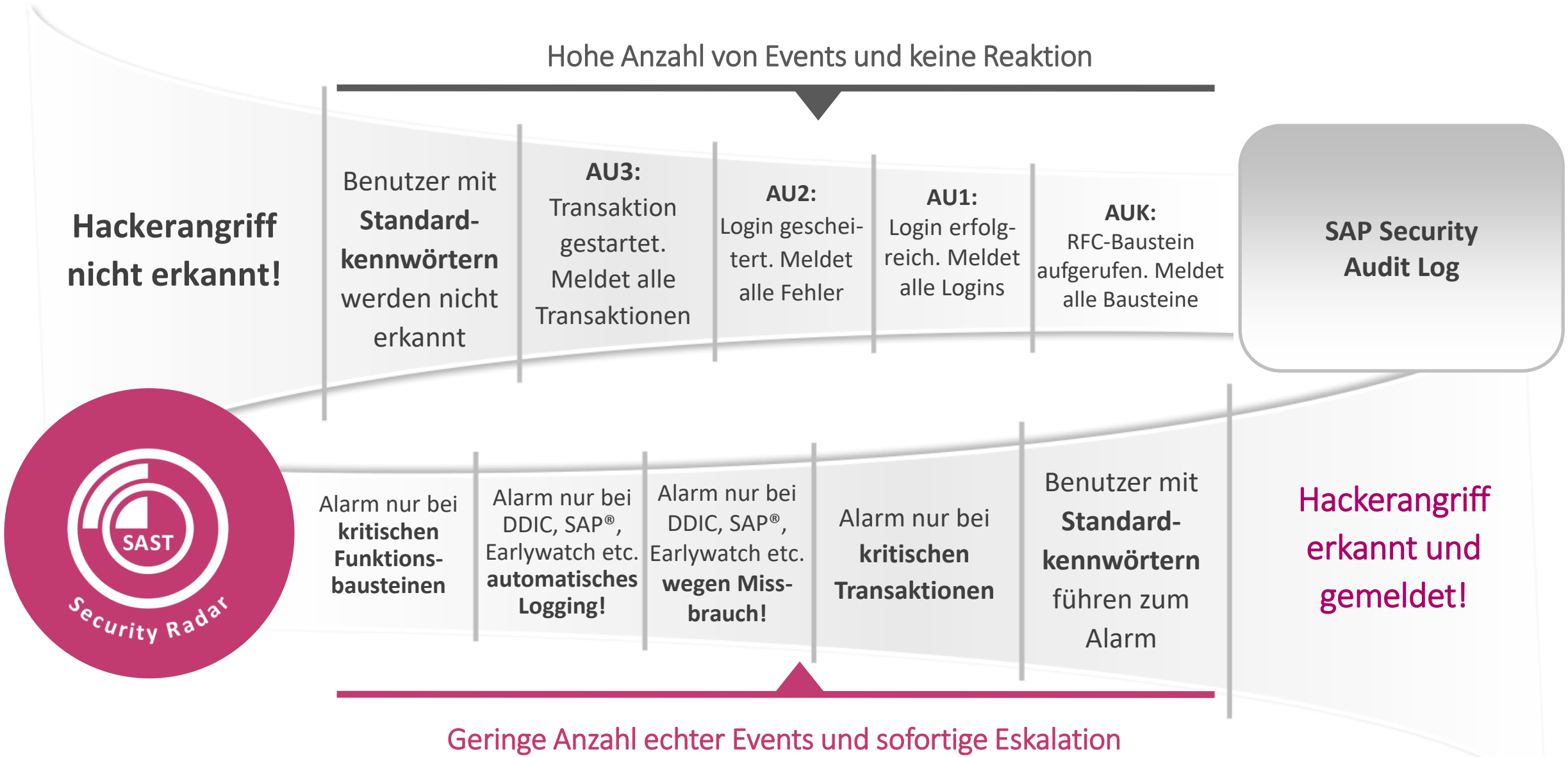
Die Herausforderung

- Gängige IT-Sicherheitslösungen binden Ihre SAP-Systeme nicht mit ein.
- Schnellstmögliche Reaktionszeit im Falle einer bedrohlichen Situation.
- Identifizierung kritischer und ungewöhnliche Aktivitäten in Echtzeit.
- Schutz Ihrer SAP-Systemlandschaft vor
  - Cyberattacken
  - Spionage
  - Manipulationen
  - Rechtemissbrauch
  - Datendiebstahl

Angriffe auf SAP-Systeme bleiben häufig unerkannt.

Die SAST SUITE überwacht Ihre SAP-Systemlandschaft vollumfänglich und in Echtzeit.

Überwachung Ihrer SAP-Systemlandschaft



Die Herausforderung

- Schutz Ihrer kritischen Unternehmensdaten vor Missbrauch, Industriespionage oder Diebstahl.
- Nachvollziehbarkeit der kritischen Downloads aus den SAP-Systemen.
- Fehlende Workflows zur Behandlung von kritischen Downloads.

Der Abzug von Daten aus dem SAP-System ist in der Regel kaum nachzuvollziehen.

Mit der SAST SUITE protokollieren Sie jeden Download.

Die Herausforderung

- Vergessene Passwörter können zur Kostenfalle werden:
  - Zeitinvestment für das manuelle Zurücksetzen eines Passworts oder eine Neubeantragung
  - Ressourcenbindung
  - Technische Kosten und Administration
- Sicherheitsrisiko durch ungenügende Passwortprozesse.

Ein Reset von Passwörtern kann in der Administration schnell teuer werden.

Mit der SAST SUITE setzen User ihr Passwort selbst zurück!

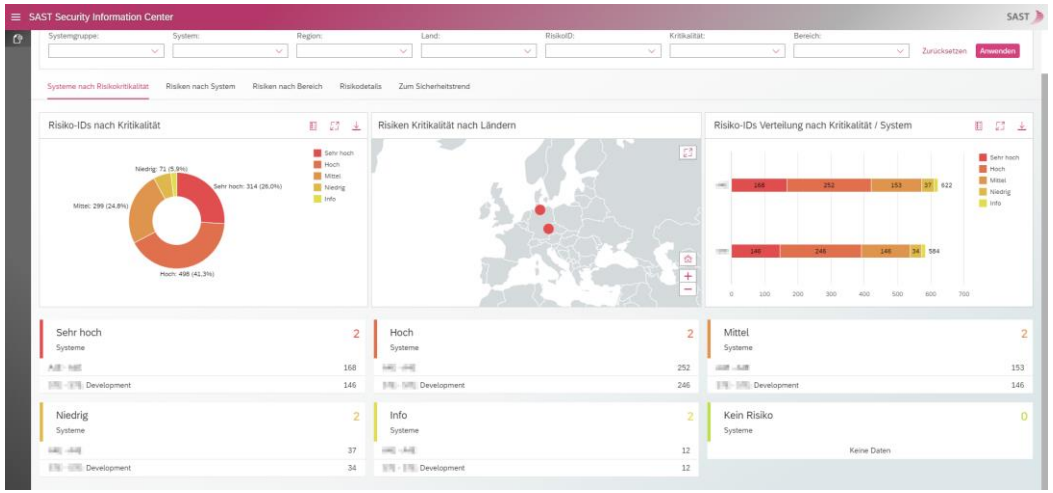
Das SAST Security Information Center

Anwendungsbeispiele

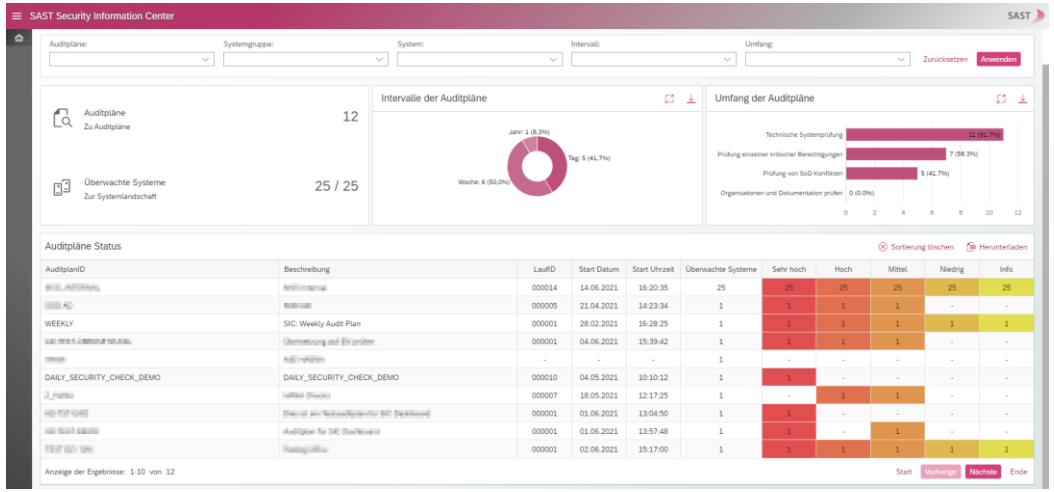
SAP-Security Configuration Monitoring

- Zentrale Übersicht über den Security-Status aller Systeme
- Jederzeit aktuelle Daten und Informationen entsprechend Ihrer internen Auditstrategie.
- Trendanalyse zur Sicherheitslage

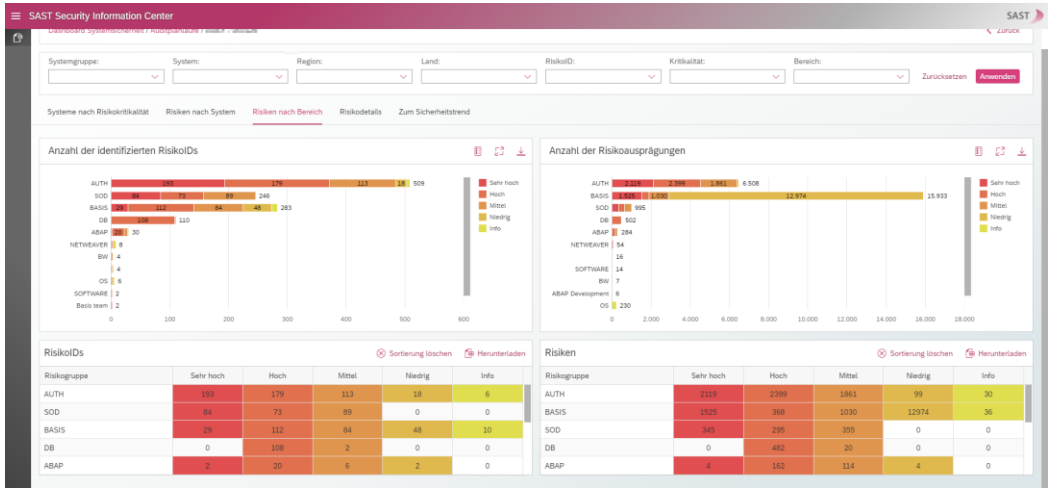
Sicherheitsstatus Ihrer Systeme auf einen Blick



Detailinformationen zu Ihren Auditplänen

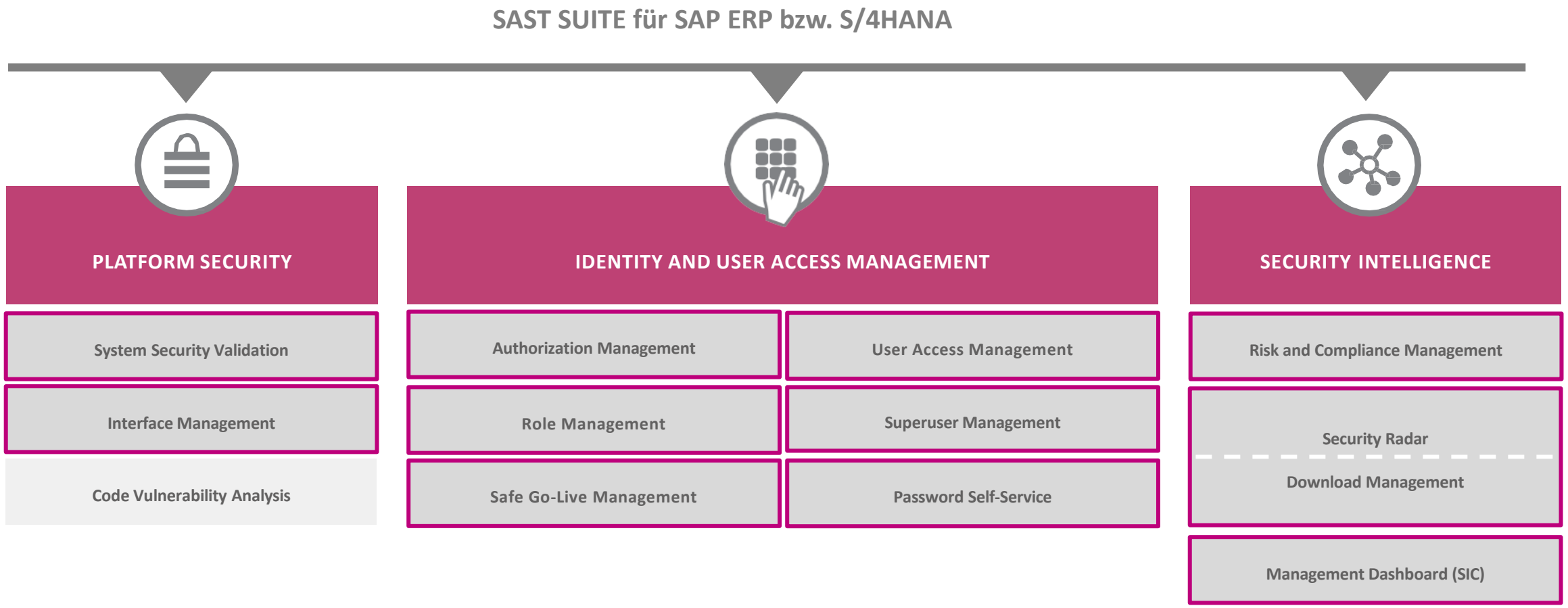


Risiken nach Bereichen



Ganzheitliche SAP Security mit SAST

- Nachfolgende Module der SAST SUITE sind bei BWB erfolgreich im Einsatz:



SIE HABEN FRAGEN?
WIR ANTWORTEN. MIT SICHERHEIT.

ANDREAS KIRSCHNER
Managing Director
Akquinet HKS business technologies

Mobil: +43 676 9398 444
E-Mail: andreas.kirschner@akquinet.at
Web: akquinet.at

CHRISTOPHER KOBALD
Senior Consultant
Akquinet HKS business technologies

Mobil: +43 676 9398 570
E-Mail: christopher.kobald@akquinet.at
Web: akquinet.de