PUBLIC

Sicher unterwegs
mit SAP’s Security Cloud Applikationen

Anna Otto, Steffen Trumpp
SAP Deutschland SE & Co. KG

9. Mai 2023

THE BEST RUN SAP

Haftungsausschluss

Die Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere sind die SAP SE oder ihre Konzernunternehmen in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen. Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen der SAP SE oder ihrer Konzernunternehmen können von der SAP SE oder ihren Konzernunternehmen jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.

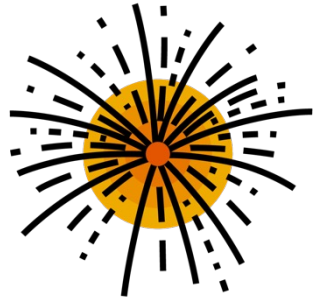
SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

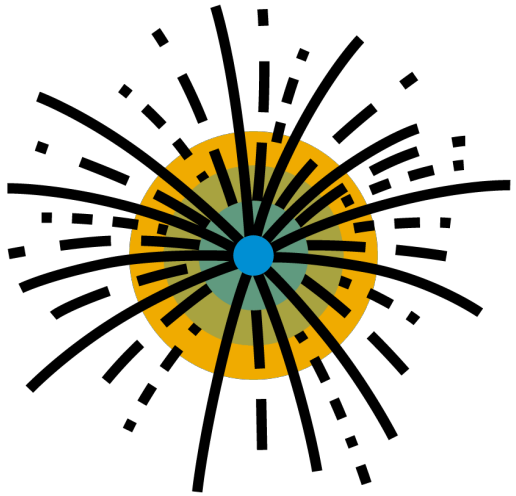
Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite www.sap.com/corporate/de/legal/copyright.html.

Agenda

- SAP GRC - NEWS
- Regelkonforme Berechtigungen mit Cloud App von SAP
- Angriffe auf SAP-Systeme im Schlaf erkennen
- One more thing
- Q&A

SAP GRC - NEWS





Ankündigung des nächsten Releases von
SAP Access Control, SAP Process Control und SAP Risk Management

- Neue Version der SAP GRC-Plattform: **SAP GRC, Edition für SAP HANA**
- Geplant für Q1 2026
- Verlängerung der Standard-Wartung SAP GRC 12 bis auf 2028
  um genügend Zeit für den Wechsel zu geben
- Müheloser Upgrade-Pfad von SAP GRC Version 12.0 auf SAP GRC Edition für SAP HANA

Weitere Details: https://launchpad.support.sap.com/#/notes/3326989

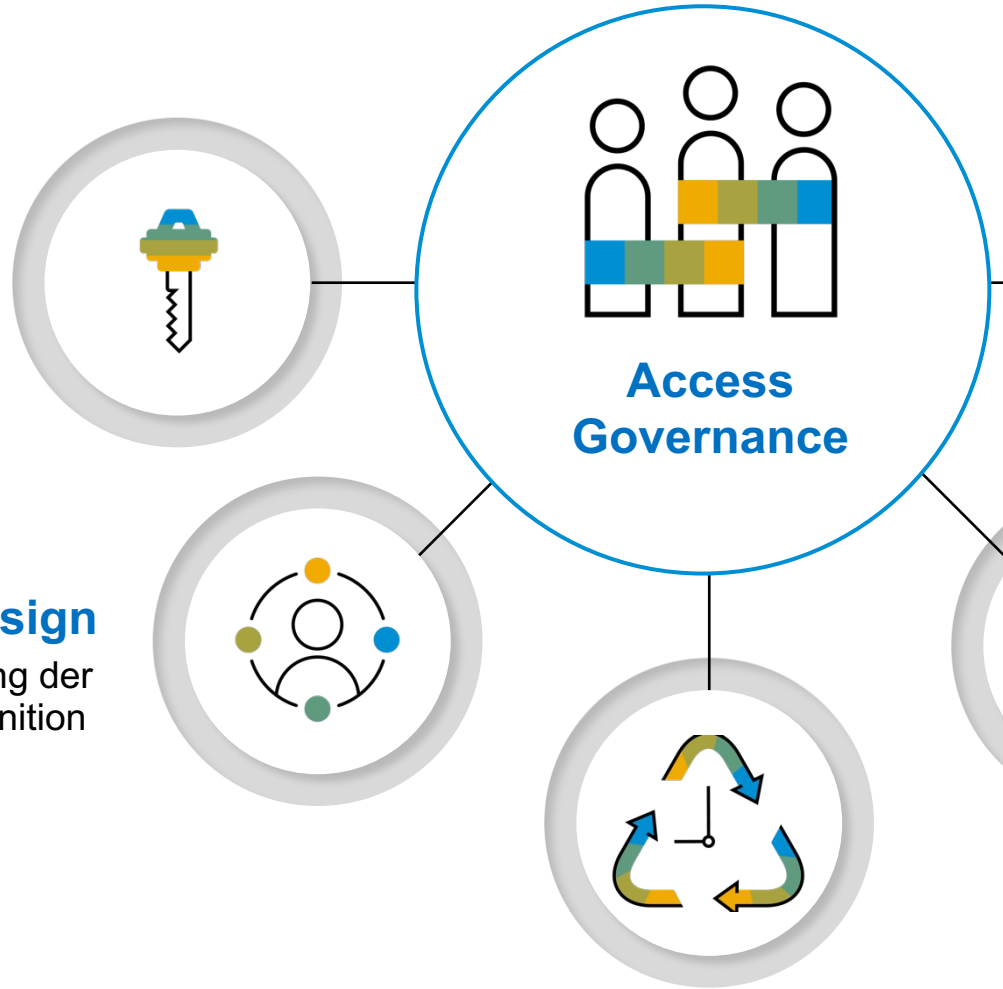
Der Inhalt dieser Folie und des Hinweises kann jederzeit und ohne vorherige Ankündigung von SAP geändert werden. Die Informationen in dieser Folie und diesem Hinweis stellen keine Zusage, kein Versprechen oder keine rechtliche Verpflichtung zur Auslieferung von Material, Code oder Funktionen dar. Diese Folie und der verlinkte Hinweis dient zu Informationszwecken und dürfen nicht in einen Vertrag eingebunden werden.

SAP Cloud Identity Access Governance

Regelkonforme Berechtigungen mit Cloud App von SAP

SAP Cloud Identity Access Governance

Überblick



Access Analysis

Benutzer und Berechtigungen analysieren

Privileged Access Management

Super-User Systemzugänge

Access Governance

Role Design

Optimierung der Rollendefinition

Access Certification

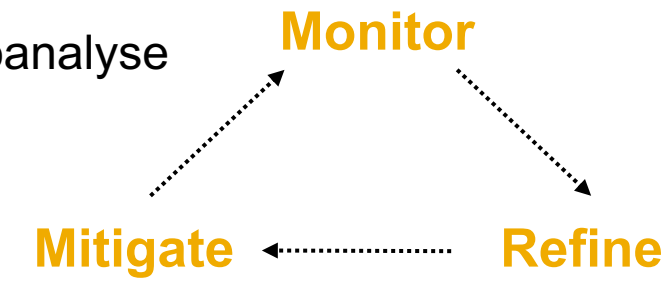
Periodische Überprüfung der Rechte und Risiken

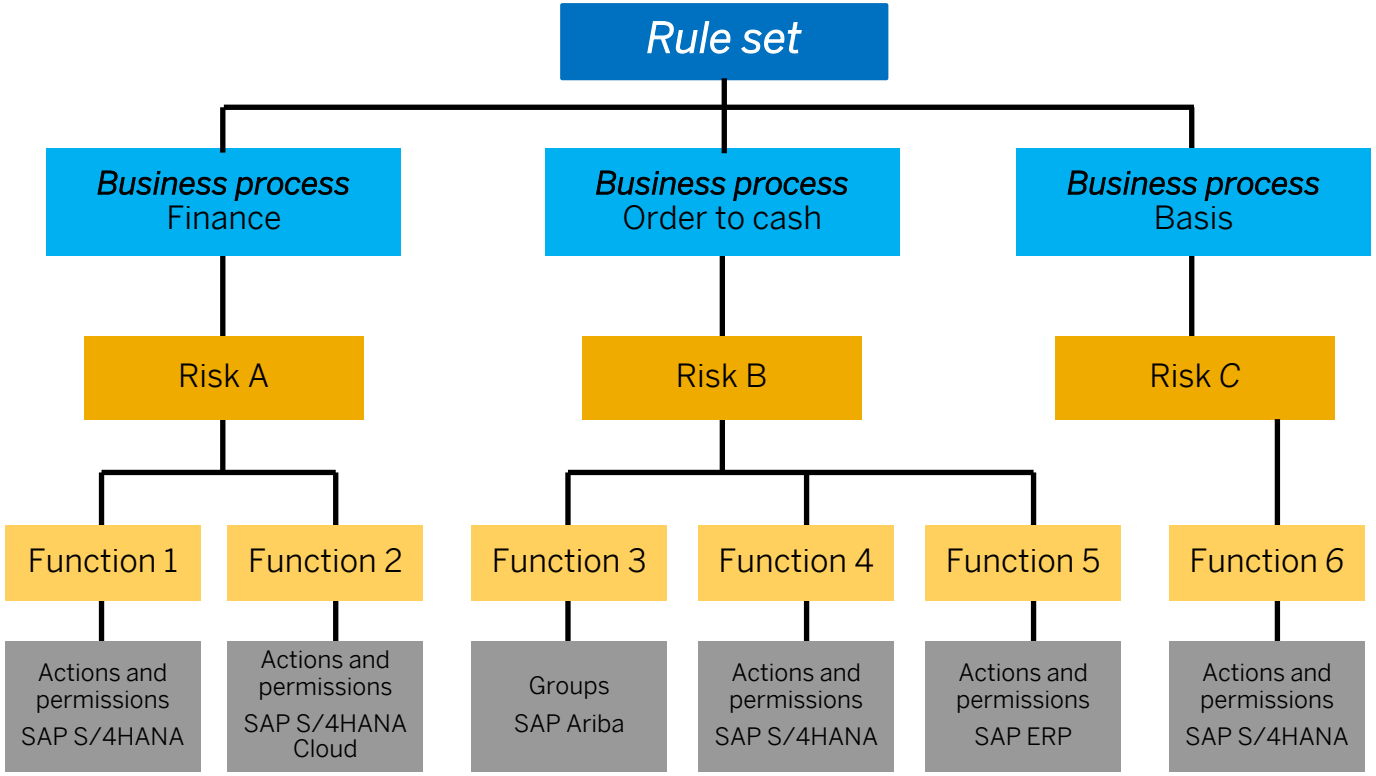
Access Request

Vereinfachung des Beantragungsprozesses

SAP Cloud Identity Access Governance

Umfangreiches, vordefiniertes Regelwerk mit systemübergreifender Risikoanalyse

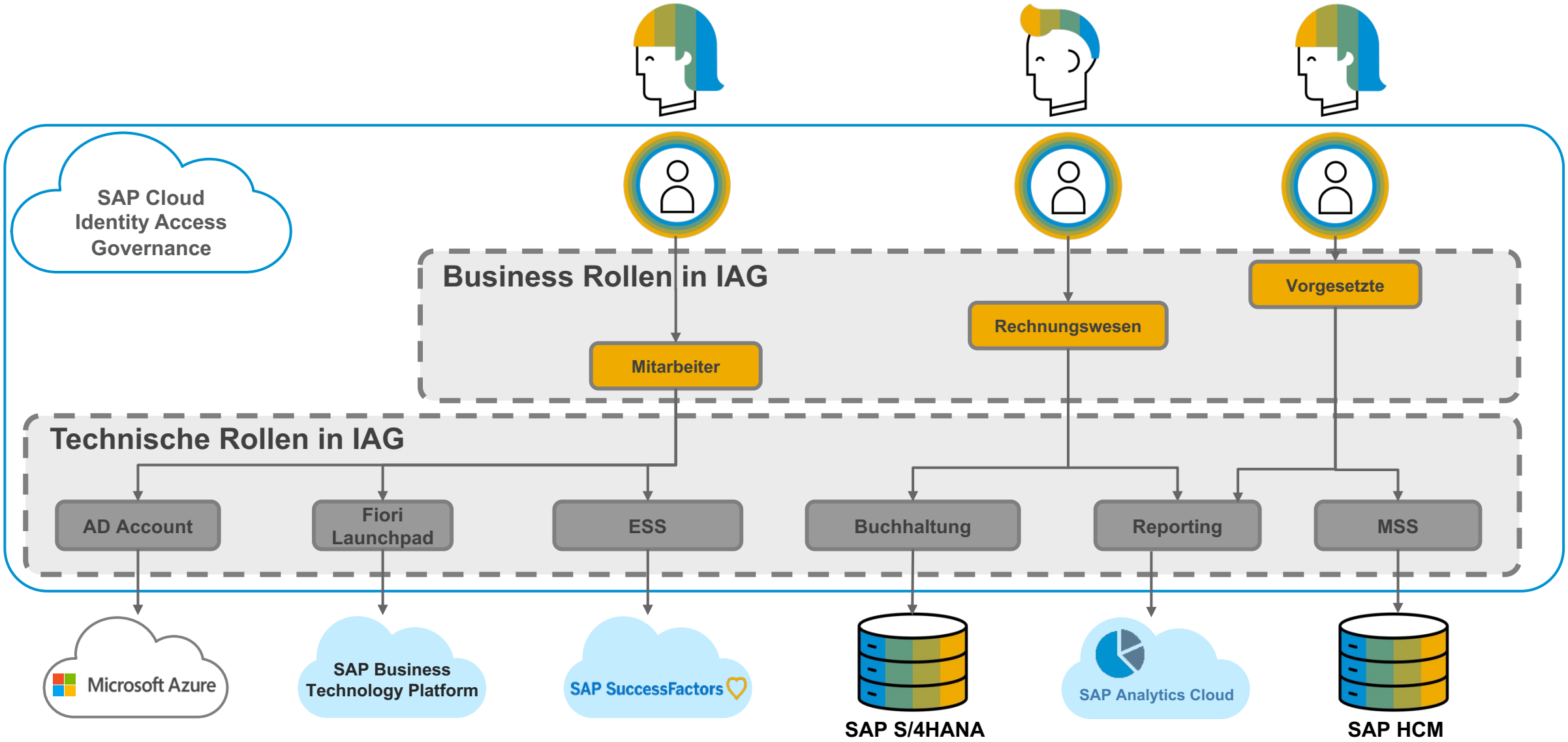




- Mehr als 500.000 kritische Berechtigungs-kombinationen (SAP's Best-Practice ruleset):
  - SAP S/4HANA & SAP ERP
  - SAP S/4HANA Cloud
  - SAP ARIBA
  - SAP SuccessFactors
  - SAP Fieldglass
  - SAP Integrated Business Planning
  - Weitere geplant

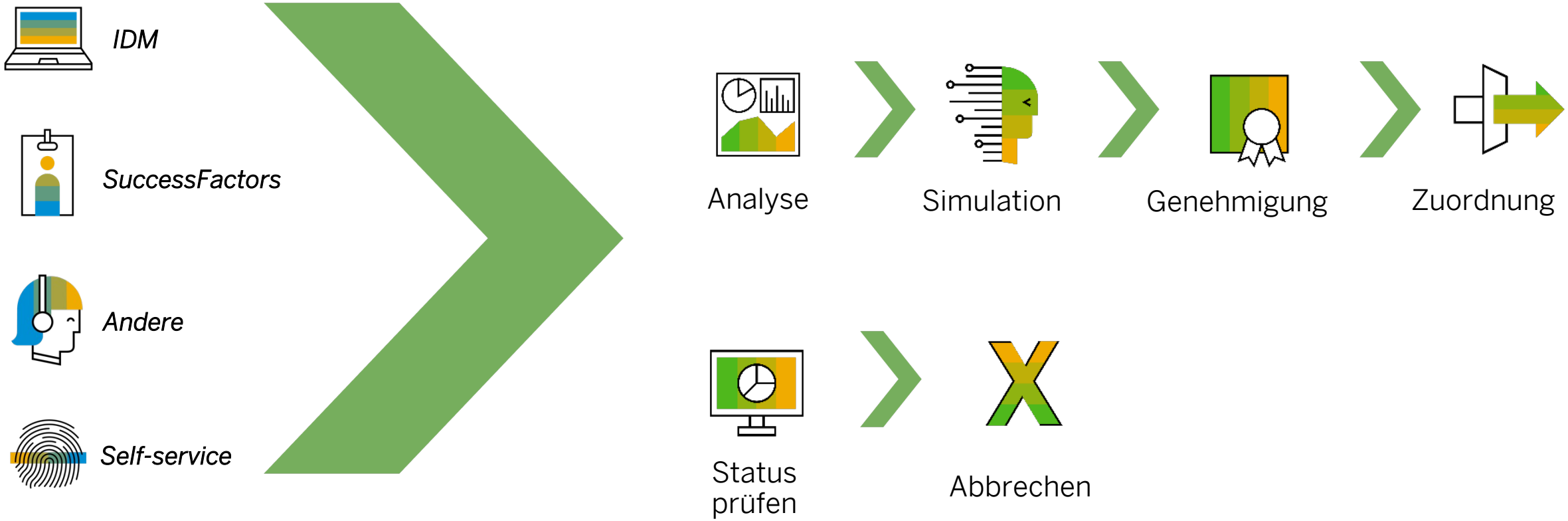
Systemübergreifende Risikoanalyse für alle Lösungen

Business Rollen Design



SAP Cloud Identity Access Governance

Workflow mit Risikoanalyse bei der Beantragung oder regelbasierten Zuordnung von Zugriffen



SAP Cloud Identity Access Governance

Zertifizierungsprozess mit Workflow zur periodischen oder ad-hoc Überprüfung von Zugriffen

Review von Rollenzuordnungen:

- Automatischer periodischer Review-Workflow von Rollenzuordnungen
- Aktuell zugeordnete Rollen werden den Vorgesetzen zum Review geschickt
- Vielfältige Selektionsmöglichkeiten der für den Review relevanten Benutzer

Geplant:

- Review von Rollen
- Review von Risiken
- Review von mitigierenden Kontrollen

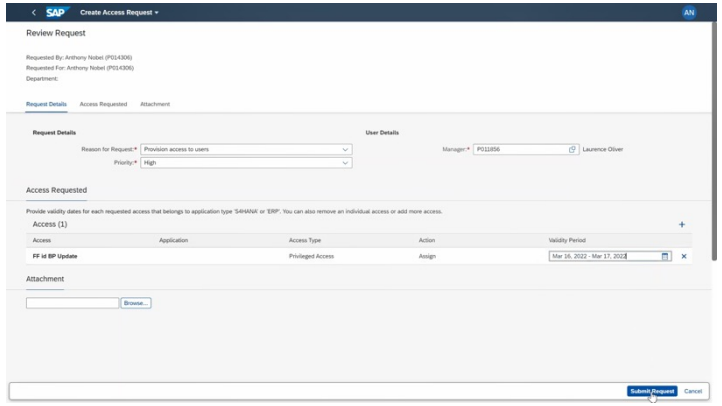
SAP Cloud Identity Access Governance

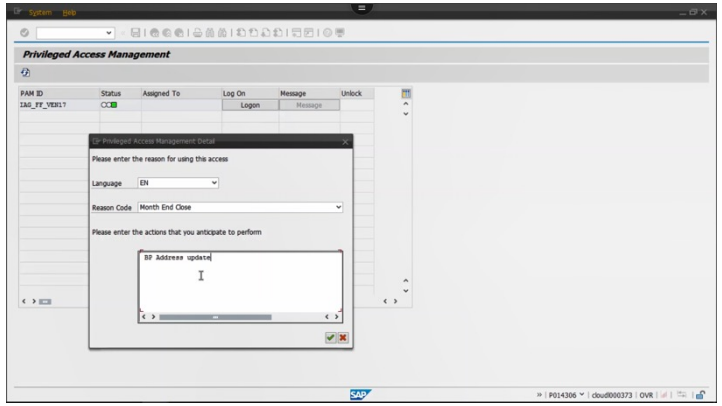
Vordefinierter auditierbarer Standardprozess für Privileged Access Management

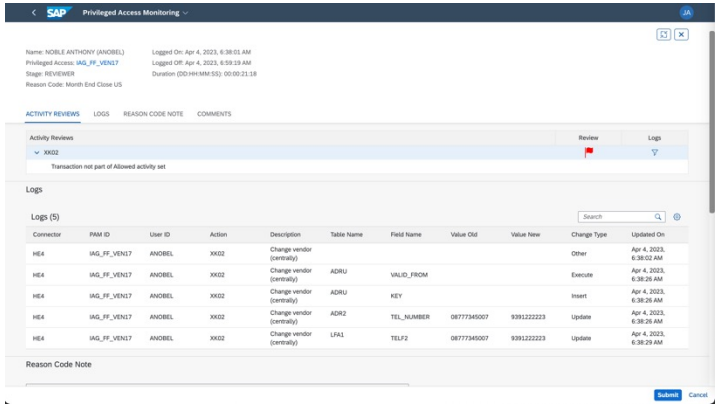
Privileged Access zuordnen

Privileged Access Sessions

Review Protokolle







Risikoeinschätzung im Antragsprozess und automatische Zuordnung nach Genehmigung

Temporärer Zugriff mit umfangreicheren Berechtigungen

Proaktive Benachrichtigungen zu kritischen Zugriffen oder ungewöhnlichen Aktivitäten

SAP ETD Cloud

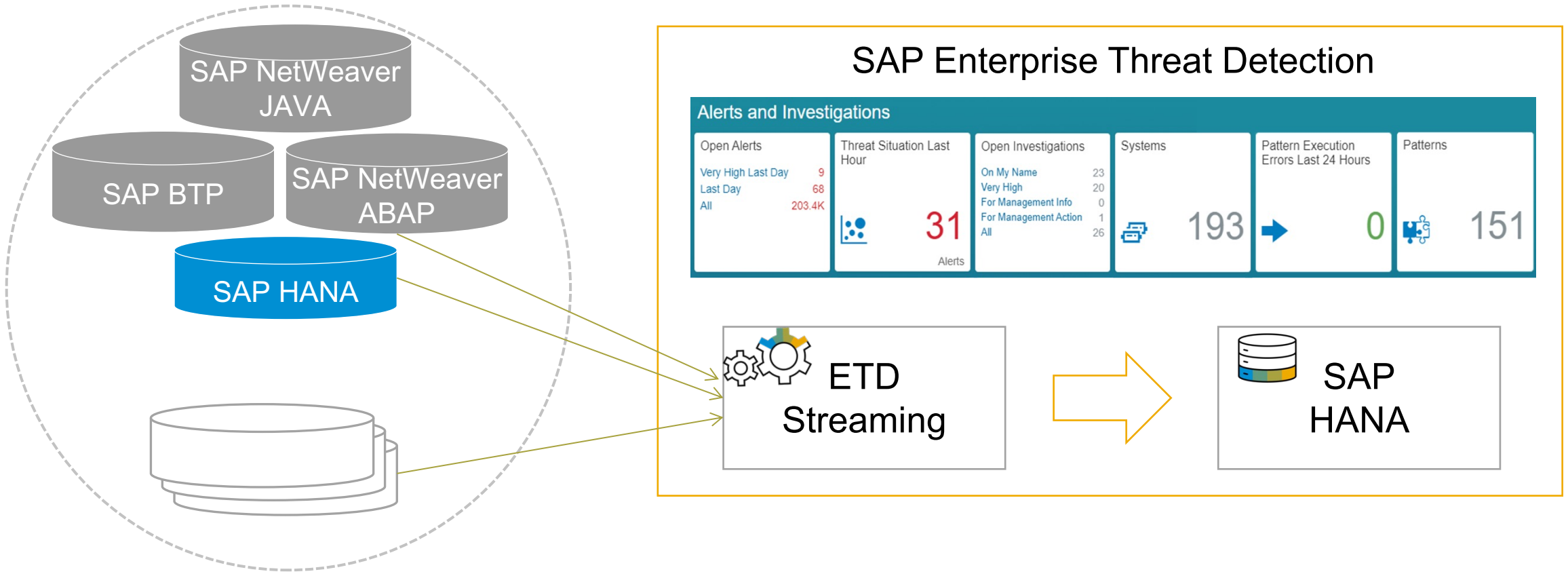
Angriffe auf SAP-Systeme im Schlaf erkennen

Ein kleiner Auszug von tatsächlichen Securityvorfällen im SAP Umfeld

- Informationen über neue Produkte wurden im Internet veröffentlicht,
  bevor das Produkt offiziell vorgestellt wurde. Die Daten lagen in SAP Systemen
- Unterbrechung von Geschäftsprozessen für mehrere Tage
  nachdem ein externen Mitarbeiter eine SAP Tabelle gelöscht hat
- Angreifer versucht über einen SAP Standard Nutzer auf die SAP Systeme
  eines Unternehmens zuzugreifen
- Herunterladen von Rezepturen aus einem ERP Test System durch einen Angestellten,
  der dann zu einem Wettbewerber gewechselt ist
- Presse publiziert Gehalt und Reisekosten des CEO
- Privilegierter Benutzer manipuliert sein Gehalt

Schützen Sie die wichtigsten Daten im Unternehmen

Architektur von SAP Enterprise Threat Detection (ETD)



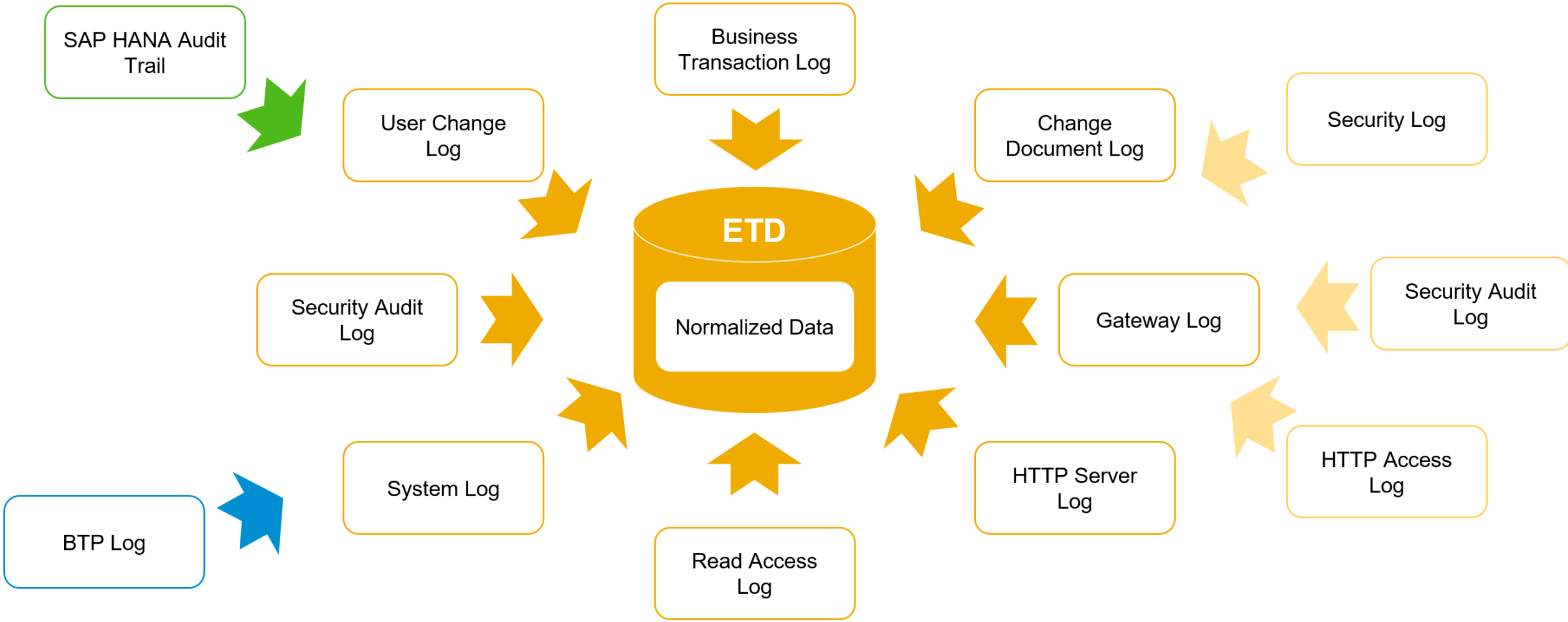
Systeme stellen Logdaten und Kontextinformationen zur Verfügung.

Auswertung in Echtzeit nur durch ETD

Normalisierung und Pseudonymisierung der Logdaten

Analyse Werkzeug
Mit 151 Standard Patterns und eigenen Analysen

SAP logs in SAP Enterprise Threat Detection



SAP ETD in der Expertensicht

Monitoring

Monitoring
Desktop Recommended

System Monitoring
Desktop Recommended

Security Notes
Desktop Recommended

41

Pattern Executions Last 24 Hours

Failed	0
All	4.1K

Pattern Executions

Pattern Execution Errors Last 24 Hours

0

Alerts and Investigations

Open Alerts

On My Name	0
Very High Last 24 Hours	0
Last 24 Hours	12
All	455

Alerts

Threat Situation Last Hour

1

Alerts

Open Investigations

On My Name	0
Very High	0
For Management Info	0
For Management Action	1
All	2

Investigations

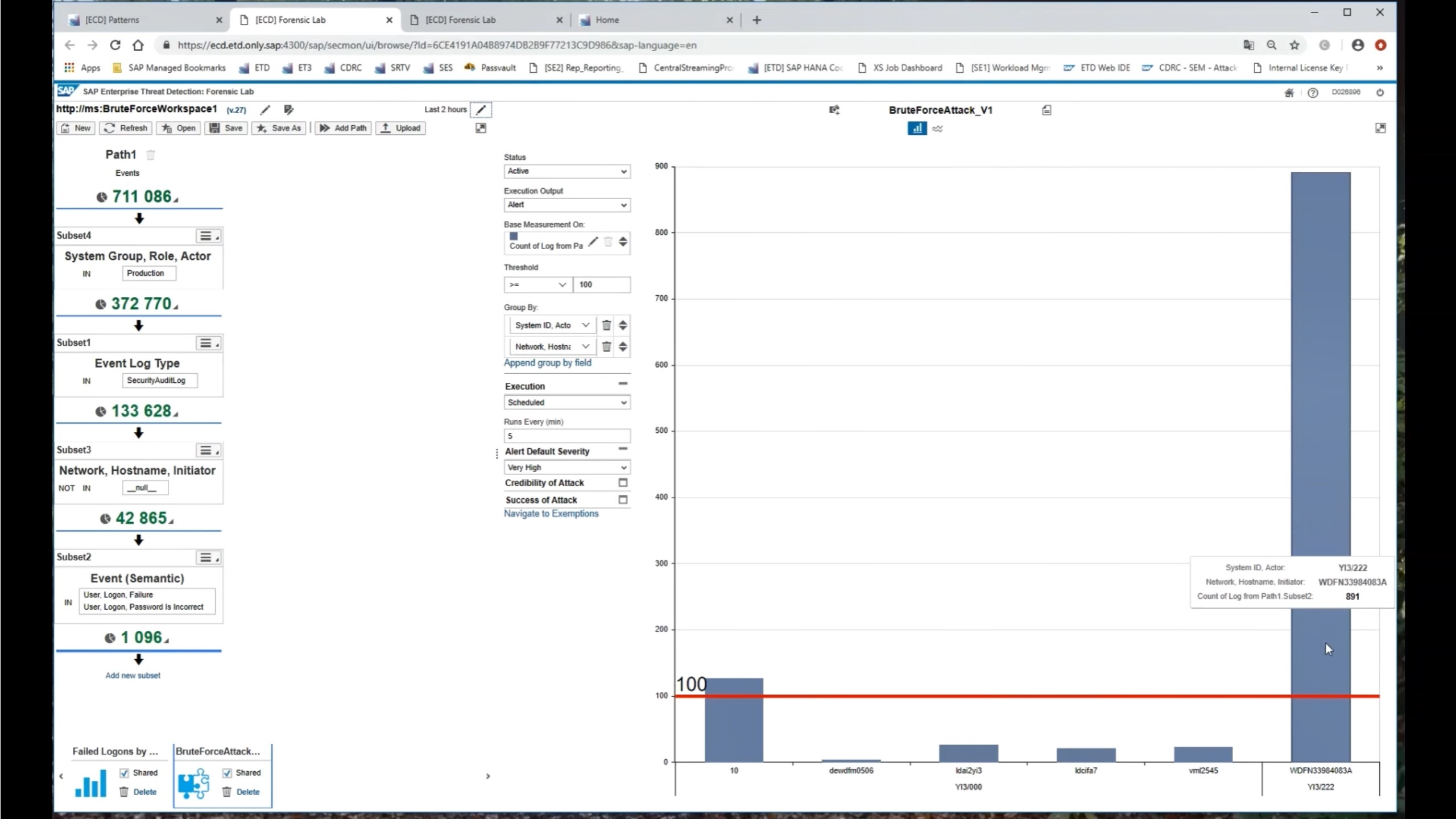
Systems
Mobile Friendly

12

Log Events Last 15 Minutes
Full Screen

Exemptions

0


[ECD] Patterns
[ECD] Forensic Lab
[ECD] Forensic Lab
Home
https://ecd.etd.only.sap:4300/sap/secmon/ui/browse/?id=6CE4191A04B8974DB2B9F77213C9D986&sap-language=en
SAP Enterprise Threat Detection: Forensic Lab
http://ms:BruteForceWorkspace1 (v.27)
Last 2 hours
New
Refresh
Open
Save
Save As
Add Path
Upload
Path1
Events
711 086
Subset4
System Group, Role, Actor
IN
Production
372 770
Subset1
Event Log Type
IN
SecurityAuditLog
133 628
Subset3
Network, Hostname, Initiator
NOT IN
__null__
42 865
Subset2
Event (Semantic)
IN
User, Logon, Failure
User, Logon, Password Is Incorrect
1 096
Add new subset
Status
Active
Execution Output
Alert
Base Measurement On:
Count of Log from Pa
Threshold
>=
100
Group By:
System ID, Acto
Network, Hostna
Append group by field
Execution
Scheduled
Runs Every (min)
5
Alert Default Severity
Very High
Credibility of Attack
Success of Attack
Navigate to Exemptions
BruteForceAttack_V1
900
800
700
600
500
400
300
200
100
0
100
System ID, Actor: YI3/222
Network, Hostname, Initiator: WDFN33984083A
Count of Log from Path1.Subset2: 891
10
dewdfm0506
ldai2yi3
YI3/000
ldcifa7
vml2545
WDFN33984083A
YI3/222
Failed Logons by ...
Shared
Delete
BruteForceAttack...
Shared
Delete

[ECD] Patterns | [ECD] Forensic Lab | [ECD] Forensic Lab | Home

https://ecd.etd.only.sap:4300/sap/secmon/ui/browse/?id=6CE4191A04B8974DB2B9F77213C9D986&sap-language=en

Apps | SAP Managed Bookmarks | ETD | ET3 | CDRC | SRTV | SES | Passvault | [SE2] Rep_Reporting | CentralStreamingPro | [ETD] SAP HANA Co | XS Job Dashboard | [SE1] Workload Mgm | ETD Web IDE | CDRC - SEM - Attack | Internal License Key

SAP Enterprise Threat Detection: Forensic Lab

D026896

http://ms:BruteForceWorkspace1 (v.27)

Last 2 hours

New | Refresh | Open | Save | Save As | Add Path | Upload

Path1

Events

711 086

Subset4

System Group, Role, Actor

IN Production

372 770

Subset1

Event Log Type

IN SecurityAuditLog

133 628

Subset3

Network, Hostname, Initiator

NOT IN __null__

42 865

Subset2

Event (Semantic)

IN User, Logon, Failure
User, Logon, Password Is Incorrect

1 096

Add new subset

Path2

Events

711 086

Subset1

Network, Hostname, Initiator

= WDFN33984083A

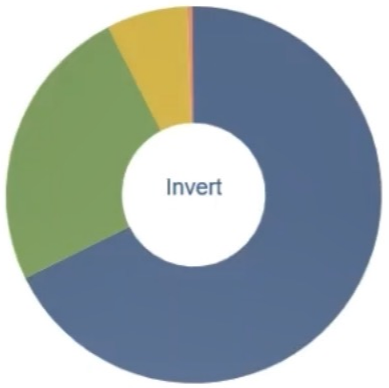
1 447

Add new subset

Distribution of Path2.Subset1 by

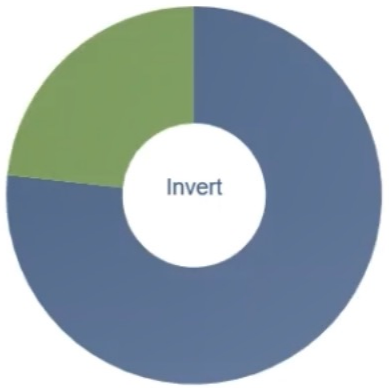
Event, Log Type

SecurityAuditLog(980)
BusinessTransactionLog(358)
Indicator(101)
SAPKernel(6)
ReadAccessLog(2)



System ID, Actor

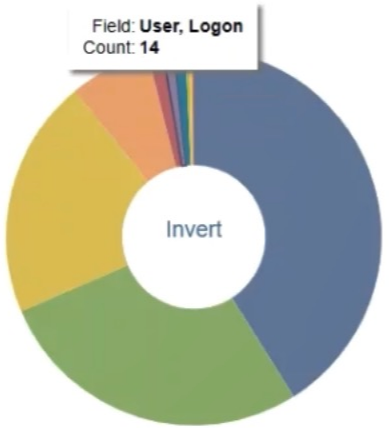
YI3/222(1110)
YI3/000(337)



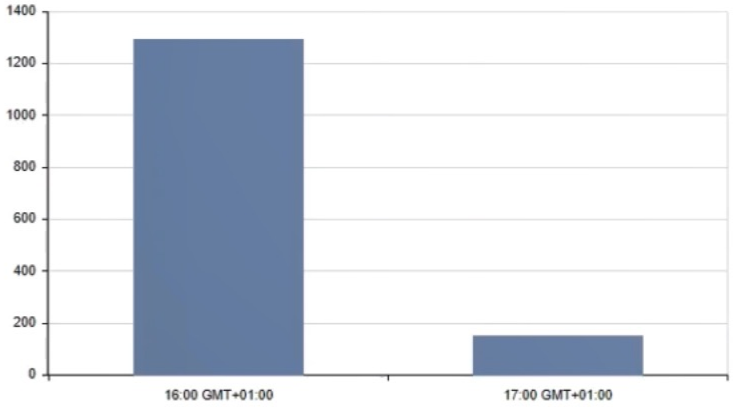
Event (Semantic)

Field: **User, Logon**
Count: **14**

User, Logon, Password Is Incorrect(594)
Executable, Run(398)
User, Logon, Failure(297)
Indicator From Pattern(101)
__null__(19)
User, Logon(14)
Execute, RFC-enabled Function Module, Run(1
Data, Download(4)
User, Logoff(4)
Data, Monitored Data, Access(2)



Timestamp



Failed Logons by ... | BruteForceAttack...

Shared | Delete | Shared | Delete

Schützen Sie die wichtigsten Daten im Unternehmen

Schützen Sie die wichtigsten Daten im Unternehmen

- SAP Experten übernehmen das SAP Security Monitoring
- Festpreis
- Regelmässige Berichte
- Benachrichtigungen bei Zwischenfällen

Schützen Sie die wichtigsten Daten im Unternehmen

Produkt beinhaltet einen Managed Service

Hacker

Kunde

Auditor / Stakeholders / Gesetzgebung

Basis Service

- ✓ 24 x 7 Warnungen
- ✓ Risko-basierte und priorisierte Untersuchungen
- ✓ Umfassendes Set von SAP Standard Patterns beinhaltet
- ✓ Monatlicher Bericht aller Vorfälle und der zugehörigen Logfiles

Rechenzentrum in Deutschland*

Sprache: Englisch

* Weitere auf Anfrage verfügbar

Schützen Sie die wichtigsten Daten

Hacker

Kunde

Auditor / Stakeholders / Gesetzgebung

Extended Service**

- ✓ Festgelegte Antwortzeiten
- ✓ Individuell vereinbarte Security Analysen
- ✓ Kundenspezifische Service Level Agreements

Basis Service

- ✓ 24 x 7 Warnungen
- ✓ Risko-basierte und priorisierte Untersuchungen
- ✓ Umfassendes Set von SAP Standard Patterns beinhaltet
- ✓ Monatlicher Bericht aller Vorfälle und der zugehörigen Logfiles

Rechenzentrum in Deutschland*

Sprache: Englisch

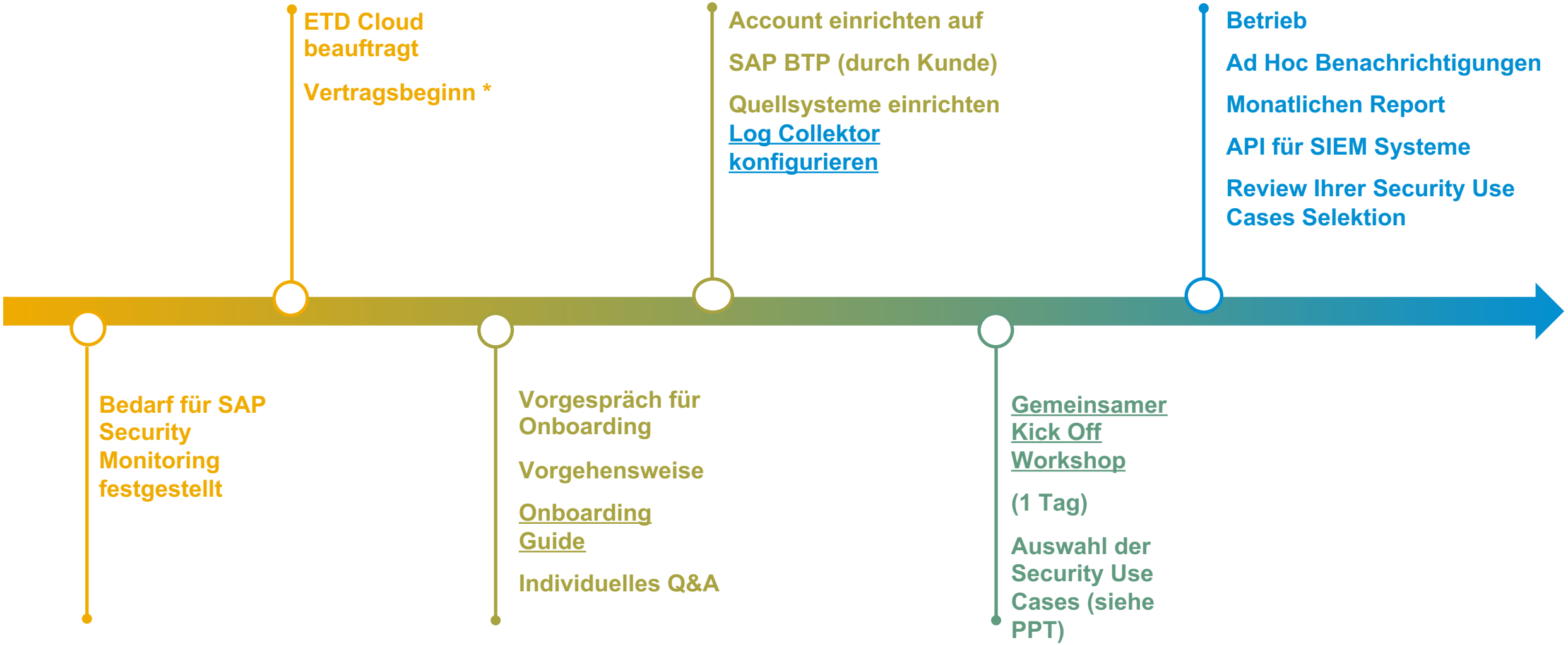
* Weitere auf Anfrage verfügbar

** Geplant für H2 2023

Aktuelle Liste der Use Cases

- Blacklisted function modules in productive systems
- Blacklisted reports in productive systems
- Blacklisted transactions in productive systems
- Blacklisted ABAP HTTP Url paths
- Suspicious Activity in Client 066
- Critical authorization assignment
- Authorization assignment by non-admin-group user
- Assign user to ADMIN user group
- User role create or drop
- User role changed to *
- Reference user assignment
- Assign user to admin group (not ABAP group)
- Client independent queries via debugger
- Critical RFC Callbacks For UserMgmt
- Data Download with Suspicious Filename
- Debugging using ABAP in Eclipse
- Debugging using new ABAP debugger
- Debugging using old ABAP debugger
- Debugging with change of control flow while debugging
- Debugging with change of variable values during debugging
- Dynamic program execution
- Failed logon by RFC/CPIC call
- Failed logon with too many attempts
- Failed logon of same user from different Terminal IDs
- Failed Logon with too many password logon attempts
- Failed Logon with expired user
- Failed Logon with locked user
- RFC-Generic table access
- Password changed for SAP standard users
- Logon with SAP standard users
- Logon success same user from different Terminal IDs
- Logon to client 066
- Password changed multiple times for same user
- Password changed by non-admin user
- User acts under created user
- User morphing by changing user type
- Table dropped or altered
- Too many selects
- Generic access to critical database tables
- Assignment of HR Critical Role to User
- Change of HR Critical Role
- Change of HR Critical Role Alternative
- Change of HR Critical Role Dynpro
- Change of Security Policy

Mein Weg zu ETD Cloud



* SAP benötigt 4 Wochen um mit dem Baseline Security Service zu starten


WEB-SEMINAR mit Anwendungs-Bericht
der KAESER KOMPRESSOREN SE
Wie kann man Angriffe auf SAP Applikationen erkennen und verhindern?
Recording abrufen
THE BEST RUN
SAP

International Conference on Cyber Security & Data Protection

23 - 24 May 2023, Amsterdam, Netherlands

- Conference Website

23 – 24 May 2023, Amsterdam, Netherlands

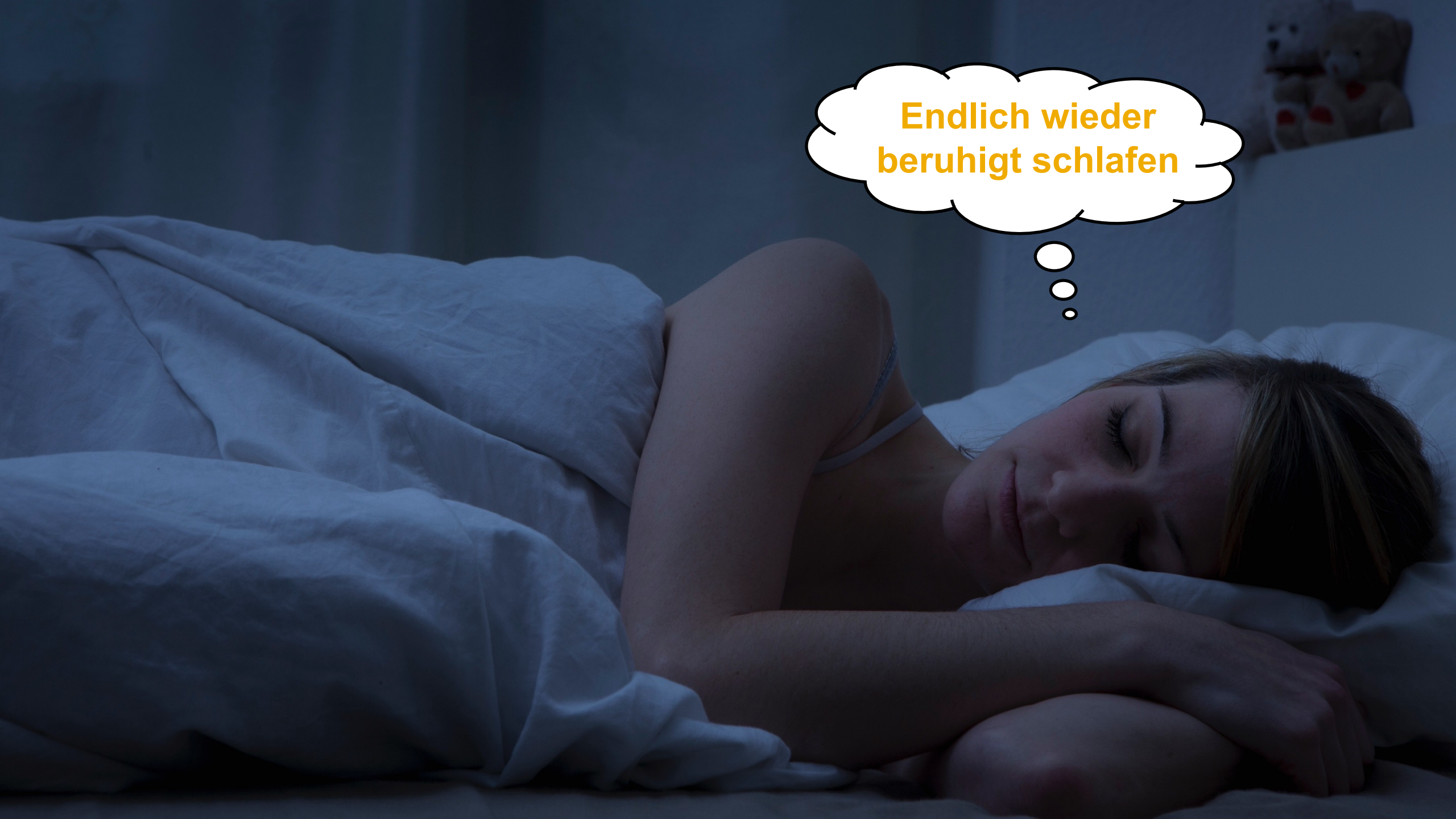
Over two days attendees will have the opportunity to hear from numerous global SAP customers, partners and the SAP experts themselves. We will be coming together to explore how leading organizations, with the help of SAP, are building robust security measures to identify, analyze, and neutralize cyberattacks in their applications as they happen and before serious damage occurs.

Attendees and speakers will share how they are protecting their growing databases and building a robust cybersecurity framework, integrating it into their existing ecosystems.

New for 2023, this year's conference will be co-located with the International SAP Conference on Internal Controls, Compliance & Risk Management. The two events will be exploring industry synergies with shared keynotes and a combined exhibition allowing extended networking for our attendees and more. As part of your ticket, you will have the opportunity to move freely between both agendas.

ETD Cloud

ETD


Endlich wieder
beruhigt schlafen

One more thing

SAP Secure Login Service for SAP GUI

Simple and secure access for SAP GUI users

Offer single sign-on based on X.509 certificates or Kerberos technology

Protect business data with strong authentication methods

Benefit from enhanced user experience and increased productivity

Integration with existing authentication infrastructure

Integrate with your existing corporate identity provider

Alternatively use Kerberos technology, based on corporate Windows domain

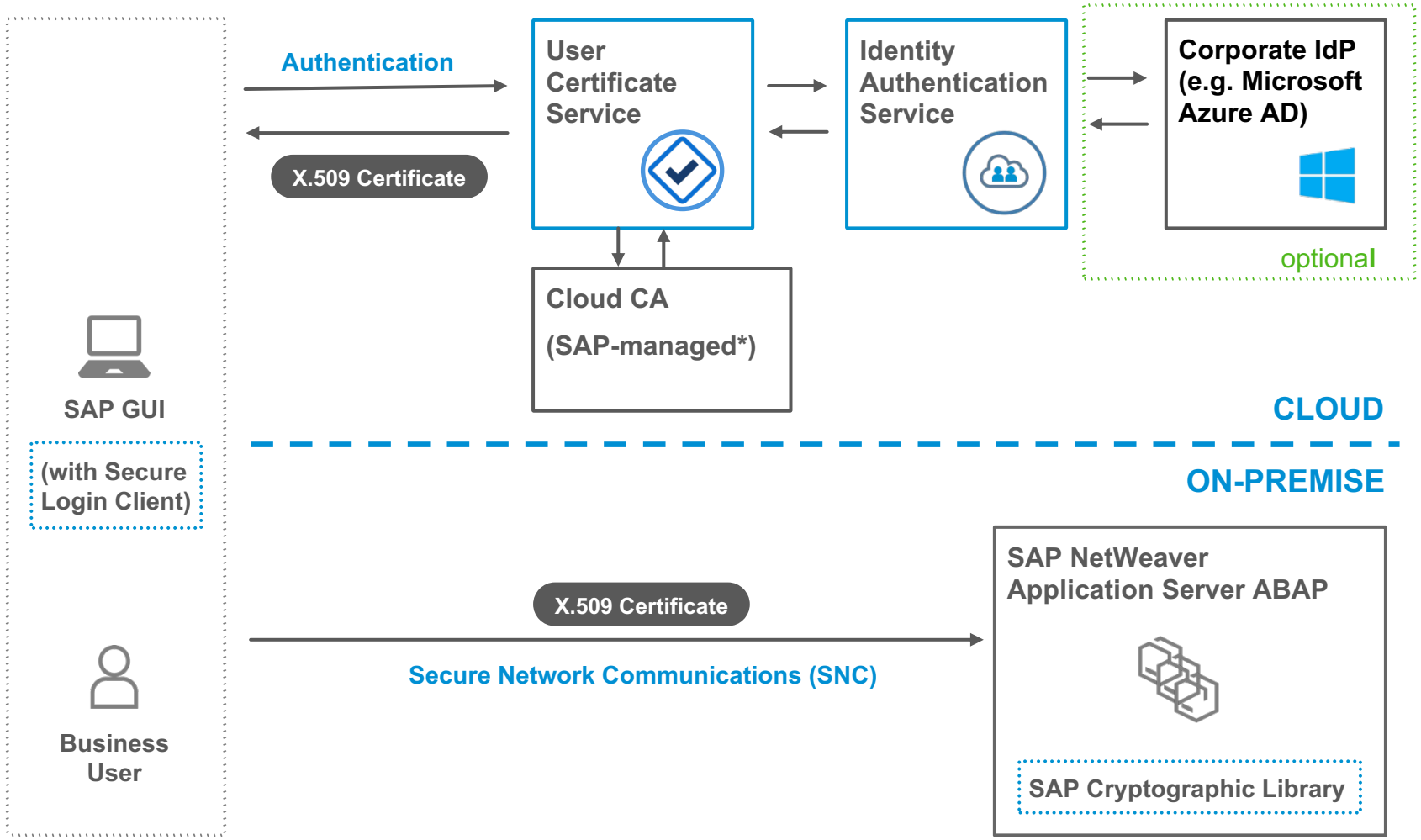
Fast implementation and low TCO

Rely on a lean cloud service

Achieve short time-to-value without any additional on-premise server components

Single sign-on based on X.509 certificates

Process flow



1. User opens a SAP GUI connection
2. Secure Login Client (SLC) redirects user to the identity provider logon page
3. User authenticates to Identity Authentication Service
4. Optionally, authentication can be delegated to a corporate IdP (such as Azure AD)
5. After successful authentication, SAP-managed* Cloud CA issues an X.509 certificate
6. User Certificate Service returns the X.509 certificate, valid for one day, to SLC
7. X.509 certificate token is used for authenticating the SAP GUI user to the ABAP system

* Support for customer-managed Cloud CA is a roadmap topic

SAP Secure Login Service for SAP GUI

Enabling single sign-on with Kerberos

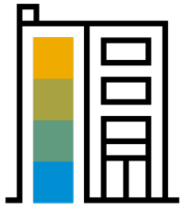
- Based on user authentication to Microsoft Windows domain during desktop login, no additional authentication required
- Microsoft Active Directory provides a Kerberos security token that SAP business applications accept as proof of identity

- Supported on Microsoft Windows and Apple macOS devices that are part of a Windows domain
- Requires the client to have access to the corporate network
- Users need to have an account in Active Directory

- Very fast implementation, very low TCO, no connectivity to cloud required
- Single sign-on for SAP GUI desktop clients

SAP Secure Login Service for SAP GUI

Positioning compared to SAP Single Sign-On



SAP Single Sign-On

Relies for capabilities such as multi-factor authentication on SAP NetWeaver Application Server Java, which will go out of mainstream maintenance end of 2027.

Includes capabilities such as an identity provider that are mostly relevant on-premise, as in the cloud there are alternatives that better fit cloud landscapes.

SAP Secure Login Service for SAP GUI

Does not rely on SAP NetWeaver AS Java, using a cloud service instead.

Focusses on the core capabilities that remain relevant even in a cloud-oriented world and adds value to these, such as an easy integration with cloud-based identity providers.

Is available as a cloud subscription, in line with how customers want to license their software today.

Where to find more information on SAP Secure Login Service for SAP GUI

Release Blog

https://blogs.sap.com/2023/05/04/sap-secure-login-service-for-sap-gui-now-available/

SAP Community

https://community.sap.com/topics/single-sign-on

Roadmap

https://roadmaps.sap.com/board?PRODUCT=AF740456A03F1EDDAA9212F748EDC3E2

Fragen? Antworten.

Steffen Trumpp
Solution Advisor Expert
SAP Security & GRC
M +49 151 57118930
steffen.trumpp@sap.com

SAP Deutschland SE & Co. KG
Tesdorpfstraße 8, 20148 Hamburg

Anna Otto
Customer Advisory Expert
Cybersecurity, Governance, Risk and Compliance

M +49 151 62345159
anna.otto@sap.com

SAP Deutschland SE & Co. KG
Tesdorpfstraße 8, 20148 Hamburg, Deutschland

Follow us

www.sap.com/contactsap

THE BEST RUN SAP