SAP Security bei der DVB Bank - Auffälligkeiten im SAP-Umfeld entdecken und Angriffe verhindern

Webcast Xiting Security Wednesday – 24.11.2021

Agenda

01/ Vorstellung DVB

02/ Überblick SAP Systemlandschaft, vor dem Projekt

03/ Problemstellung

04/ Xiting Security Architect

05/ SAP ETD

06/ Status Quo

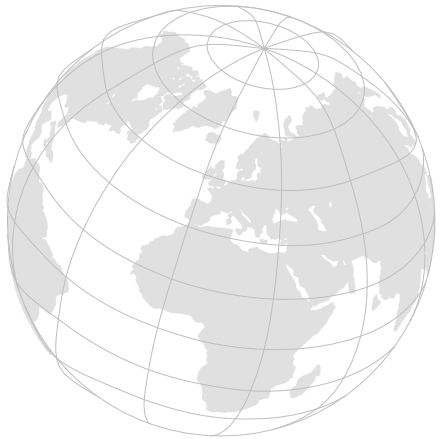
07/ Architektur – Xiting Security Architect / SAP ETD & Splunk

08/ Umsetzung mit Xiting Security Architect & SAP ETD

09/ Live-Demo

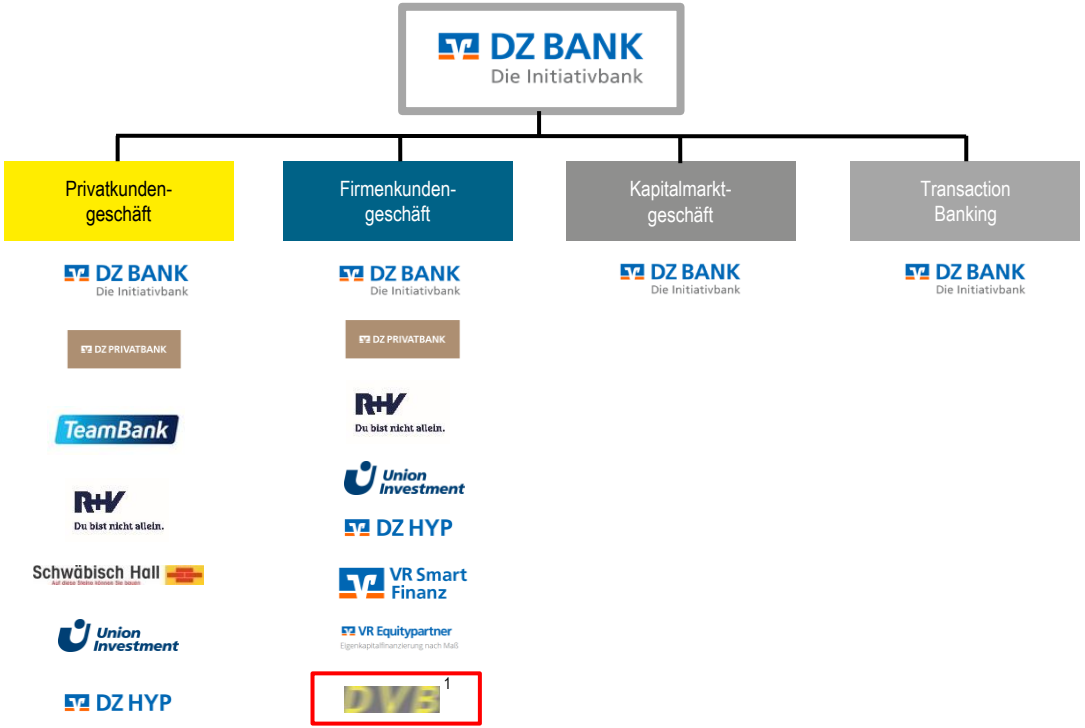
10/ Ausblick

11/ Fragen



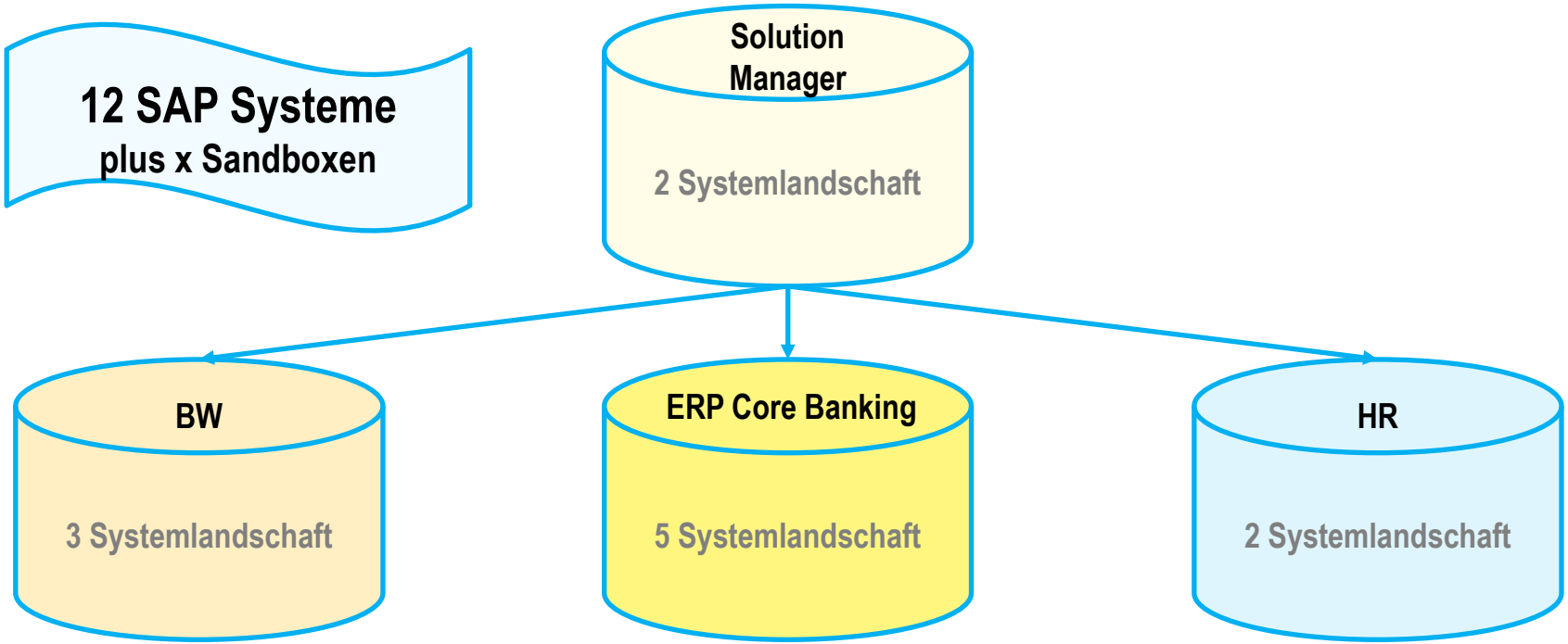
01/ Die DVB Bank gehört zu Deutschlands zweitgrößter Bankengruppe

- Der DVB Bank Konzern ist ein Finanzdienstleister, der sich auf das internationale Transport-Finance-Geschäft spezialisiert hat.
- Mit 329 Mitarbeitern und Standorten weltweit verwaltete die DVB zum 31. Dezember 2020 ein Kreditportfolio im Wert von 3,9 Mrd €.



1 Nach dem Verkauf von Kerngeschäftsfeldern im Jahr 2019 hat die DVB die Amortisierung ihrer verbleibenden Portfolien initiiert. Infolgedessen führt die Bank ihr Bestandsgeschäft als voll operational tätige Bank fort, hat aber im Bereich Shipping Finance das aktive Marketing eingestellt und schließt grundsätzlich kein Neugeschäft mehr ab.

02/ Überblick SAP Systemlandschaft, vor dem Projekt



03/ Problemstellung, früher waren Cyberangriffe auf SAP eine absolute Seltenheit

Früher war eine Firma:

- in sich geschlossen
- in einer überschaubaren Umgebung
- der Pförtner kannte alle
- die SAP Systeme waren hinter der Firewall sicher
- interne Angriffe waren selten

Einfache Schutzmaßnahmen reichten aus:

- Geschlossene Fenster, versperrte Türen, Zaun, etc.

03/ Problemstellung, heute gibt es viel mehr Cyberangriffe auf SAP Systeme

1) Heutige Ausgangslage:

- Öffnung der SAP Systeme durch Digitalisierung (Internet, Firmen Devices, offene API's, …)
- Es ist komplex SAP Systeme mit den vielen Angriffsmöglichkeiten als Gebäude gut zu schützen
- Wichtigste Daten einer Firma sind oft in SAP Systemen gespeichert
- Viele Personen haben Zugriff auf die Daten
- Angriffe auf SAP werden im Internet beschrieben, Schwachstellen werden ausgenutzt, etc.

2) Resultat:

- Angreifer haben viel mehr Möglichkeiten anzugreifen
- SAP Systeme müssen deutlich mehr geschützt werden im Vergleich zu früher

Fazit: Neue erweiterte Sicherheitskonzepte sind notwendig:

- Viele Einstellungen sind aktiv zu verwalten, Einführung vorbeugender Maßnahmen, etc.
- Eine Übersicht ist zur Kontrolle erforderlich
- Ein ständiges Monitoring über den Status der SAP Security ist notwendig geworden

03/ Problemstellung und warum ein Projekt notwendig ist

Anforderungen werden immer mehr und Ergebnisse von Revisionsprüfungen sind umzusetzen

- SAP Systeme kommen immer mehr in den Fokus von **Angreifern**
- Anforderungen der **BAFIN** durch die Veröffentlichung der **BAIT** wurden konkreter und umfangreicher
- Die **EBA** initiierten Prüfung forderten eine regelmäßige Kontrolle der Einstellungen der produktiven Systeme
- Der **DSAG-Sicherheitsleitfaden** wurde als Mindestansatz von der Revision geprüft und eine Prüfung dessen wird nun jedes Jahr vollumfänglich erwartet (hoher manueller Aufwand)
- Die **BSI** Veröffentlichungen und Gültigkeit wurden auf die SAP Systeme ausgeweitet
- Die Konzern-IT wollte Daten von den SAP-Systemen für das **SIEM** Tool
- Die jährlich durchgeführten **Pen-Test**s brachten immer öfter neue Folgeaktivitäten hervor
- Die externen **Prüfer** kamen mit mehr automatisierten und umfangreicheren Prüfungen und Anforderungen
- Alles erfordert entsprechende Dokumentationen und Nachweise

03/ Problemstellung und warum war ein Projekt notwendig geworden

➔ BAFIN, EBA, BSI, …

Neue Regularien

Neue Anforderungen

Strengere Sanktionen

➔ Hacker „entdecken“ SAP

Cyber-Kriminalität

Automatisierte Angriffe

Neue Risiken

➔ schnell reagieren

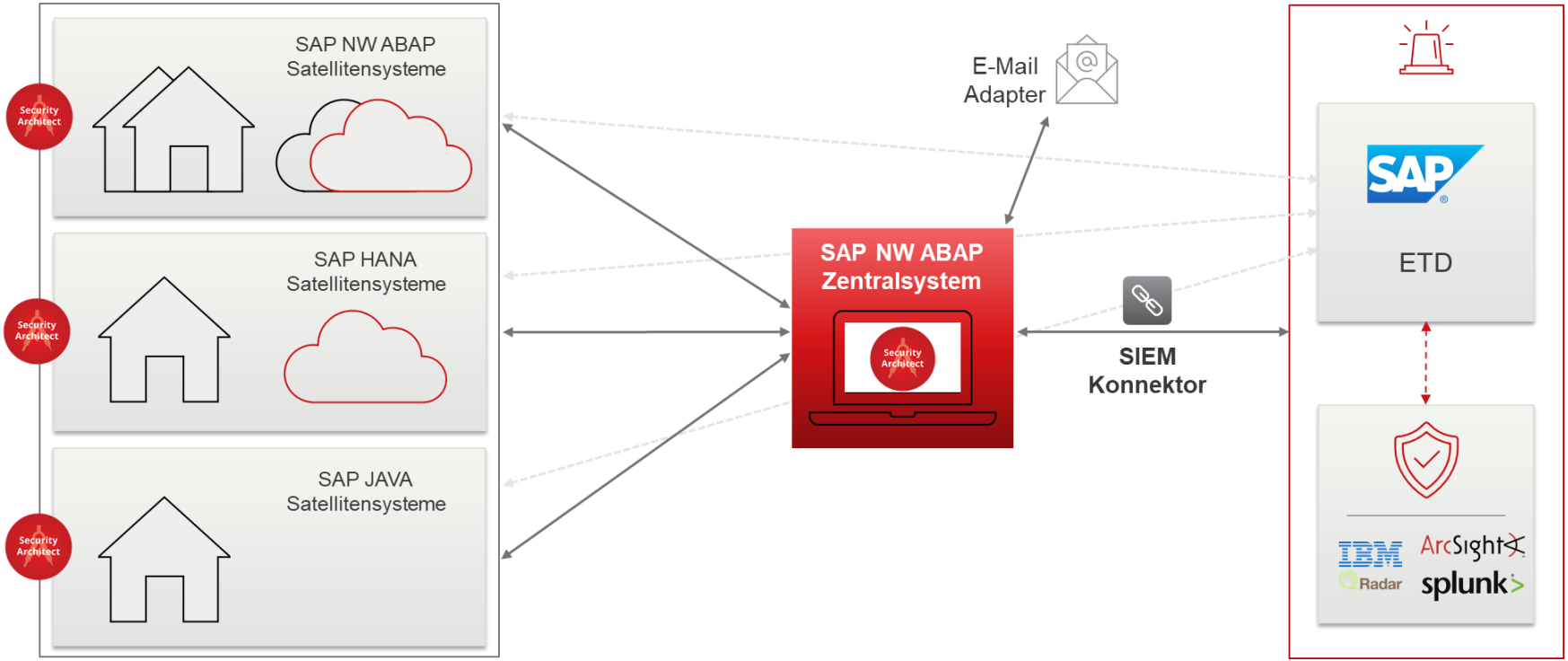
Fehlende Transparenz

Prozessautomatisierung

Neue Angriffsvektoren

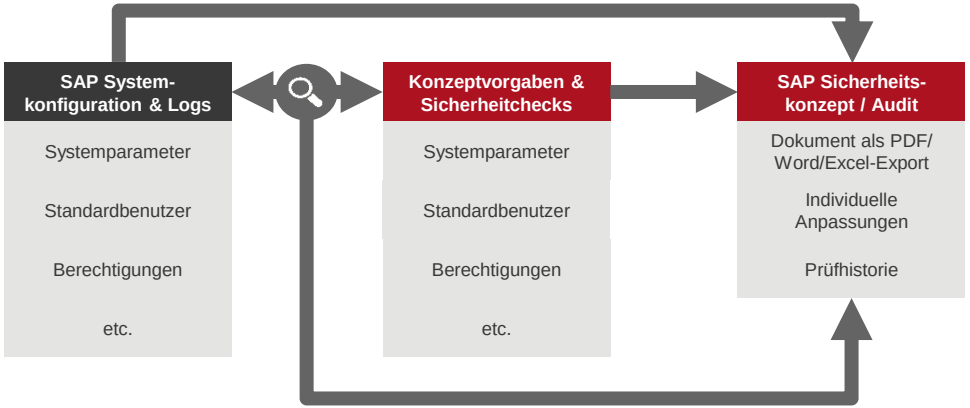
➔ All das zusammen bedeutet, dass man bis zur nächsten Prüfung viel Arbeit hat

04/ Ganzheitliches SAP Security Monitoring - Architektur



04/ Xiting Security Architect – Frühzeitige Identifikation von SAP Compliance Verletzungen

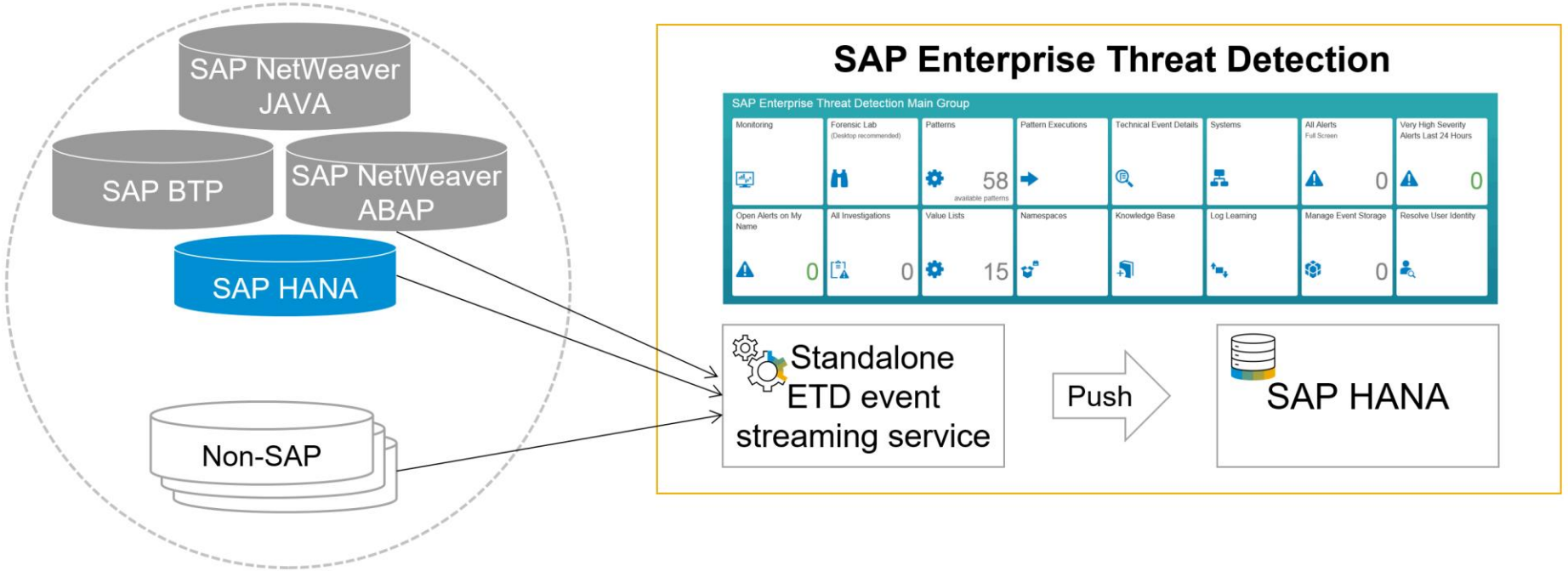
- Automatische Erstellung systembezogener Sicherheitskonzepte per Knopfdruck
  - Nutzung von best practice Vorlagen sowie Ausgabe als PDF- oder HTML-Dokument
  - Wartung und Aktualisierung von Sicherheitsrichtlinien zur Vermeidung von operativen Risiken
  - Kundenindividuell anpassbares Framework
- Prüfung des SAP Systems gegen Sicherheitsvorgaben (Monitoring und Validierung)
  - Lokale und zentrale Durchführung von Systemprüfungen (automatisiertes Compliance-Monitoring)
    - >250 vordefinierte Checks (z.B. vorkonfiguriert für Empfehlungen gemäß DSAG-Prüfleitfaden, SAP Security Baseline, GDPR)
  - Speicherung und Vergleich von Prüfergebnissen (Historie)
  - Verwaltung von Ergebnissen (Alerting & Mitigation)
- Integration und Aufbau eines ganzheitliches Security-Monitoring
  - Kontinuierliche Transparenz der Systemumgebungen
  - Integrativer Betrieb mit SAP ETD
  - Flexible und skalierbare SIEM-Integration via Log-Kollektoren



04/ Xiting SIEM-Connector– Identifizierung von unerwünschten Aktivitäten

- Konfigurierbares SIEM-Cockpit
  - Log-Extraktoren sowie erweiterbares Framework (kundenindividuelle Checks integrierbar)
  - Flexibles Ausgabe-Format je nach SIEM-System (XML, JSON, CEF)
  - Intervalle zur Überprüfung frei konfigurierbar
- Flexible SAP Log-Extraktionen
  - Vorkonfigurierte Log-Extraktoren
    (Security Audit, HANA Audit, System Log)
  - Standardisierte Schnittstelle und Konsolidierung der
    unterschiedlichen SAP-Logs
    (Benutzerdaten, Bewegungsdaten, Änderungslogs)
- Integration von Checks aus dem Security Architect
  - Zusätzliche Informationen über den SAP-Standard hinaus
  - Auswertung von Compliance-Vorgaben in Echtzeit

05/ Architektur von SAP Enterprise Threat Detection



Systeme stellen Logdaten und Kontextinformationen zur Verfügung.

Auswertung in Echtzeit nur durch ETD

Normalisierung und Pseudonymisierung der Logdaten

Analysetools

05/ Events, Pattern, Alarme und Untersuchungen

Event: User QWERT-12345 tries to log into a system, but fails.

Event: User QWERT-12345 tries to log into a system, but fails.

…

…

Event: User QWERT-12345 logs into a system.

Event: User QWERT-12345 creates a user ASDFG-67890.

Event: User ASDFG-67890 logs into a system.

Erfolgloser Login mit zu vielen Versuchen

Benutzer verwendet einen selbsterstellten Benutzer

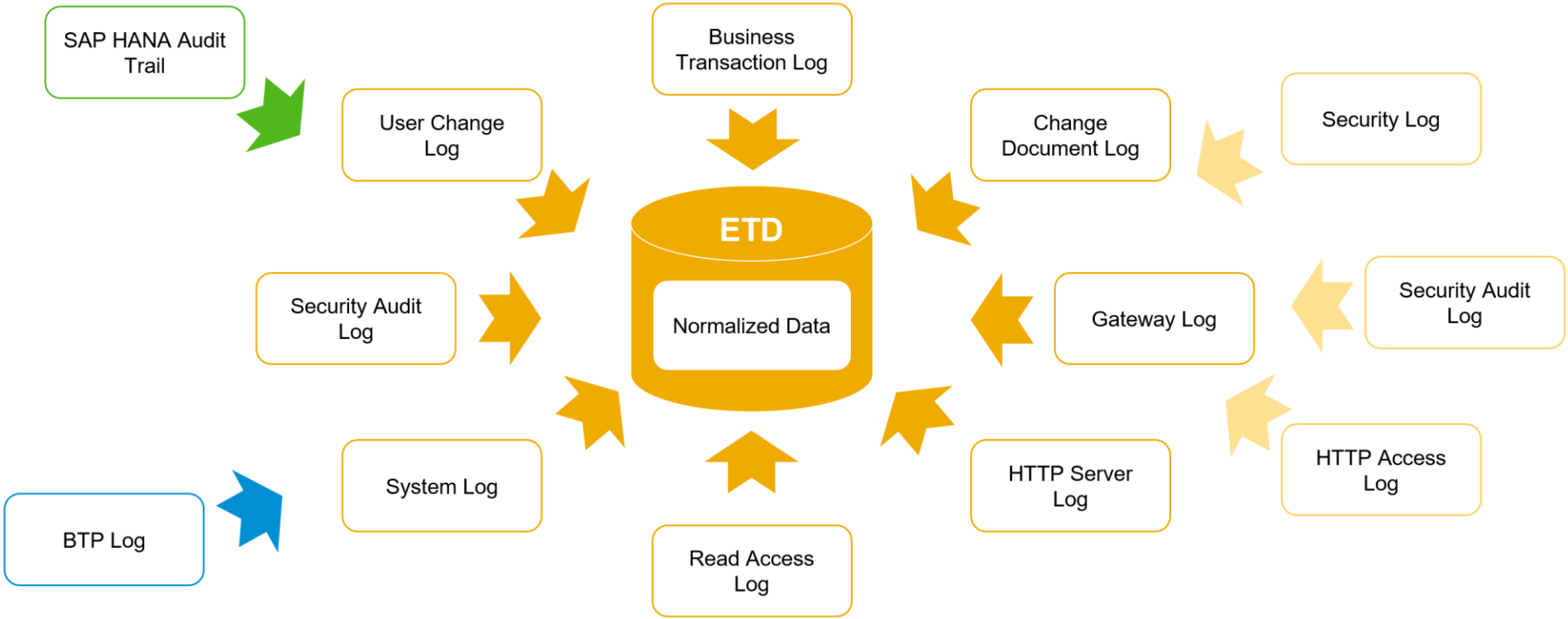
Alert 1:
Severity Low,
System XYZ,
Terminal ABC,
User QWERT-12345

Alert 2:
Severity High,
System XYZ,
Terminal ABC,
User QWERT-12345,
User ASDFG-67890

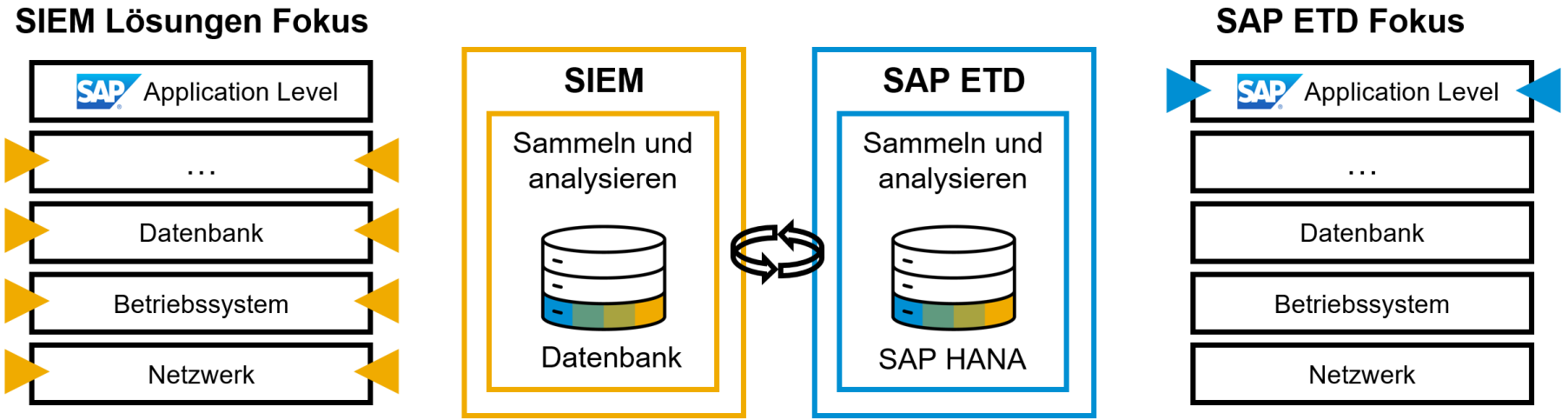
Investigation 33:

Severity High,
Status Open,
Alert 1
Alert 2
Alert …

05/ SAP logs in SAP Enterprise Threat Detection



05/ SAP Enterprise Threat Detection (ETD) und generische SIEM Systeme



Überwachung von Auffälligkeiten ohne Integration des Applikationslayers

+

Real time Monitoring von Business kritischen SAP Applikationen und Daten

Generische Integration von SAP ETD mit führenden SIEM Lösungen (Arcsight, IBM Q-Radar, Splunk, …) verfügbar

06/ Entscheidung

sich gegenseitig ergänzend

Enterprise Threat Detection

Internes Kontrollsystem

Lieferung der Daten an Splunk

Real-time Monitoring und Alarmierung

06/ Erkenntnisse im Projektablauf

1. Ziel: Anbindung der SAP Systeme an das SIEM System (Splunk) mit SAP ETD

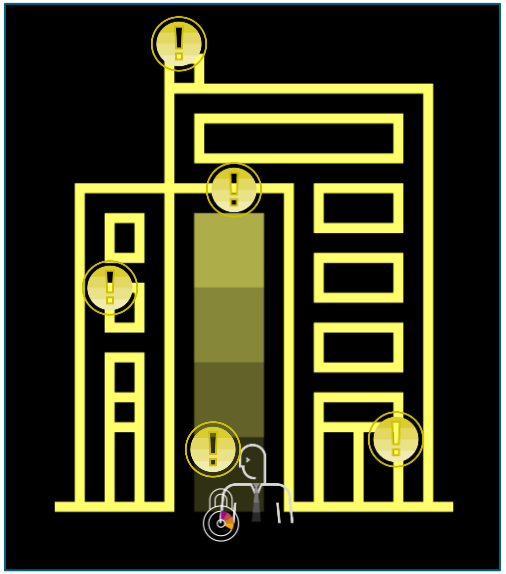
/ SIEM (Splunk) wollte alle Events aus den SAP Systemen direkt und ohne jegliche (Vor-)Verarbeitung haben

/ Der SAP ETD und Splunk Connector wurde genutzt, dafür werden die Daten sehr früh aus den SAP ETD abgezogen und auch keine Anonymisierung / Pseudonymisierung der Daten (wie in ETD üblich) durchgeführt

2. Ziel: Analyse der Events der SAP Systeme / Nachweis der regelmäßigen Prüfung

/ Unterscheidung der statischen und dynamischen Prüfung
- Im Projektverlauf wurde erarbeitet, dass die Tools Xiting Security Architect und SAP ETD für verschiedene „Zustände“ verwendet werden
- Die statischen Daten werden vom Xiting SA verwaltet und dokumentiert, wie z.B. Parameter, Überprüfung kritischer SAP Berechtigungen, kritischer Profile, SAP Standarduser oder Client Settings (SCC4)
- Die dynamischen Daten werden von SAP ETD verwaltet, wie z.B. Benutzeränderungen ohne IDM, Änderungen an Logging Einstellungen, Änderungen Profilparameter über RZ10 (RAL), Dialoganmeldung nicht-personalisierter Benutzer

06/ Verhinderung von Cyberangriffen auf SAP durch statische Analysen



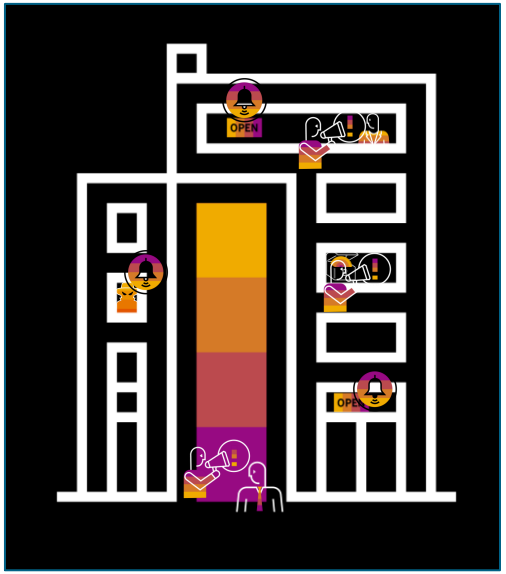
Automatische Erstellung systembezogener Sicherheitskonzepte

Regelmäßige Prüfung der Systemlandschaft

Statische Analysen sind notwendig um z.B. sicherzustellen:

- Sind die Fenster und Türen richtig geschlossen?
  - ICF-Knoten
  - RFC-Destinationen
  - Profilparameter
- Wem wurden Schlüssel ausgegeben?
  - Kritische Berechtigungen
  - Kritische Profilzuweisungen
- Sind die Kameras installiert?
  - Korrekte Logging-Einstellungen

06/ Verhinderung von Cyberangriffen auf SAP durch dynamische Analysen



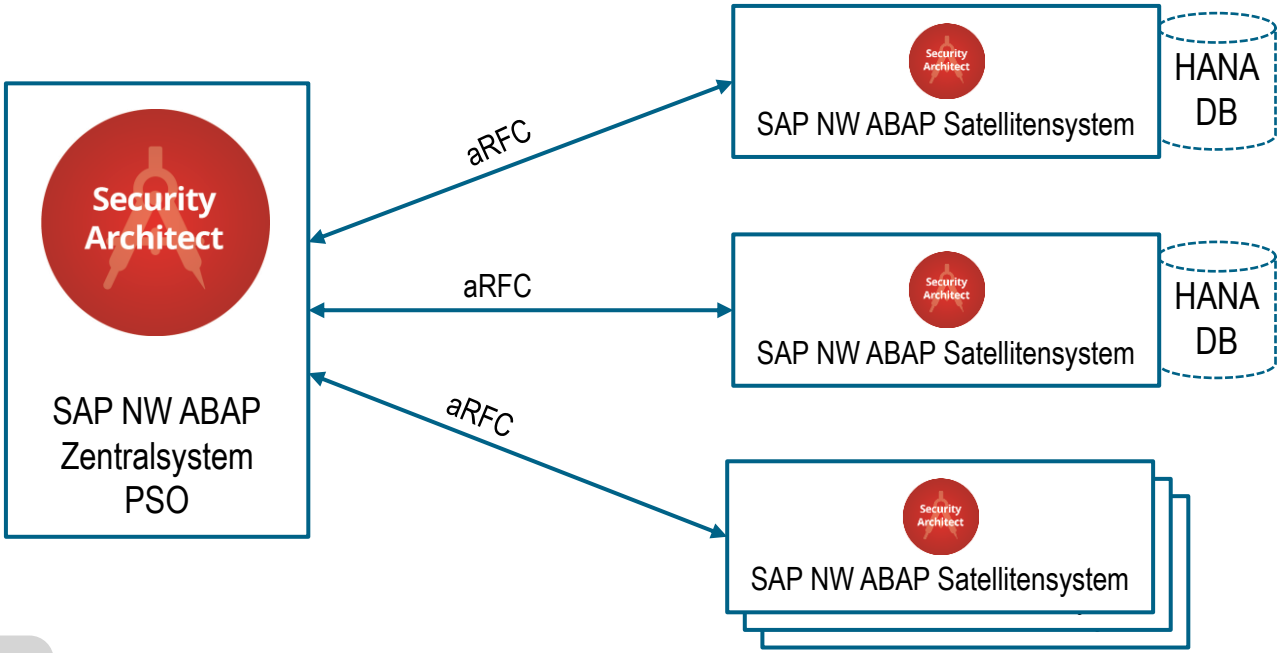
Dynamische Analysen in Echtzeit sind notwendig, um Angriffe bereits in der Vorbereitung zu erkennen.

- Alarmanlage/Brandmeldeanlage/Kamera
  - SAP Enterprise Threat Detection (ETD)
    - Temporäre Zuordnung von kritischen Berechtigungen
    - Überprüfung des Missbrauchs von nicht eingespielten Security Notes
    - Ausnutzung eines SAP Standardnutzer
- Rundgänge durch privaten Wachdienst
  - Threat Hunting via ETD
    - Untersuchung eines Alerts/Vorfalles im Unternehmen
    - Anpassung der Patterns auf kundenspezifischen Schutzbedarf

06/ Projektverlauf

- Aufgabe: Konfiguration vom Xiting Security Architect und Installation & Konfiguration von SAP ETD
- Abbildung der verschiedenen vorgegebenen „use cases“ in den Systemen
- Anbindung der SAP Systeme über SAP ETD an Splunk
- Projektdauer: ca. ½ Jahr (Testphase wegen der False-Positive großzügig wählen)

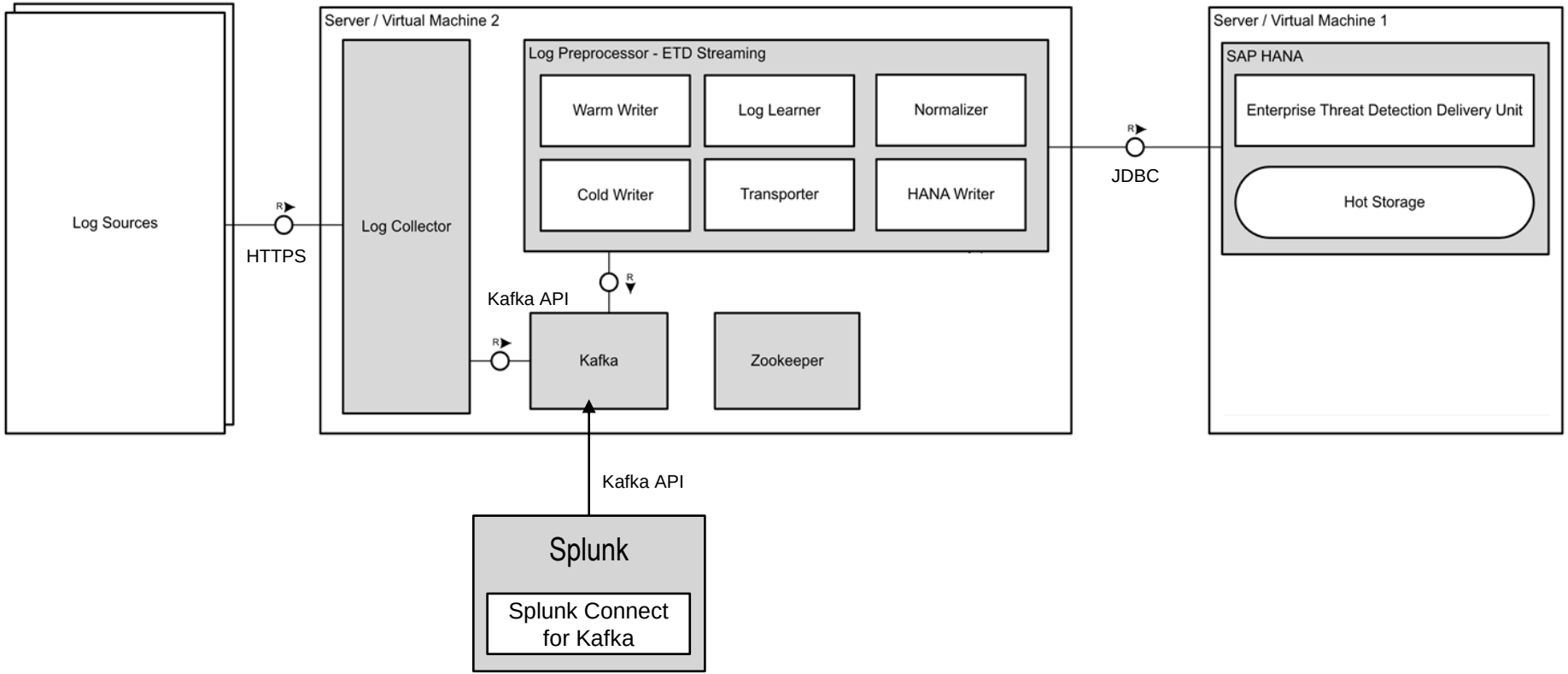
07/ Architektur – Xiting Security Architect



Legende:

- Umgesetzte Architektur
- Geplante Architektur

07/ Architektur - SAP ETD & Splunk



08/ Umsetzung mit Xiting Security Architect & SAP ETD

Aufteilung der Anwendungsfälle :

- regelmäßige und zentralisierte Überprüfung der Sicherheitseinstellungen
  - statische Konfiguration
    - Parameter, z.B. login/*; auth/*
    - Überprüfung kritischer SAP Berechtigungen, z.B. S_USR_GRP; S_DEVELOP
    - Zuweisung kritischer Profile SAP_ALL; SAP_NEW
    - RFC von nicht-produktiven zu produktiven Systemen
    - SAP Standarduser, z.B. SAP*; DDIC
    - Client Settings (SCC4)
- Erkennung und Alarmierung von Sicherheitsvorfällen
  - dynamisch
    - Benutzeränderungen, die nicht vom IDM initiiert werden
    - Änderungen an Logging Einstellungen, z.B. SAL
    - Änderungen Profilparameter über RZ10 (RAL)
    - Löschen des SAP*
    - Dialoganmeldung nicht-personalisierter Benutzer, z.B. SAP Support User

09/ Live-Demo

10/ Ausblick

“Security is a never ending story”

- Implementierung weiterer Pattern für SAP ETD
- Aktualisierte Fassung der verschiedenen Leitfäden im Security Architect abbilden
- Konzept für Mitigationen im Security Architect
- Einbindung der SAP HANA Datenbanken in den Xiting Security Architect
- GRC Regelwerk für Rollen (Kombination kritischer Berechtigungen) im Xiting importieren

11/ Fragen

Danke

Christof Awater, DVB Bank SE (Christof.Awater@dvbbank.com)
Ralf Adam, (Ralf.Adam@dvbbank.com)
Steffen Trumpp, SAP Deutschland SE & Co. KG (steffen.trumpp@sap.com)
Hendrik Heyn, Xiting GmbH (HHeyn@xiting.de)
Patrick Spitzer, Xiting GmbH (pspitzer@xiting.de)