SAP SECURITY

SAP Security Group Vienna Edition · XITING FALCORA

# SAP Security Operation & AI: Vom blinden Fleck zur vollen Sichtbarkeit

Wie Falcora SAP Security Operations sichtbar und steuerbar macht – und wo KI dabei hilft.

AGENDA

# Vom blinden Fleck zur vollen Sichtbarkeit.

Erst die Grundlagen, dann das SAP-Problem, dann die Lösung – mit einem konkreten Beispiel.

**01**

## Grundlagen

Security Monitoring kurz erklärt: NIST CSF, SIEM & SOC.

**02**

## Der blinde Fleck SAP

Warum SAP im Security Monitoring so oft fehlt.

**03**

## Sichtbarkeit mit Falcora

Wie Falcora die Lücke schließt – und wo KI hilft.

**04**

## Praxisbeispiel

Ein Alert in Falcora – von der Erkennung bis zur Eindämmung, mit Fortinet.

**05**

## Takeaways & Q&A

Was Sie morgen anders machen können.

TEIL 1 · GRUNDLAGEN

# Was ist eigentlich SAP Security Monitoring?

Ein Rahmen, zwei Bausteine – und warum SAP darin so oft fehlt.

01

# It’s time to fall in love with SAP logs




*Because they tell you everything — if you understand them*

© 2026 Xiting AG. All rights reserved

WHAT IS SECURITY MONITORING?

# A risk-based framework — NIST CSF 2.0.

NIST CSF 2.0 organizes cyber risk into six functions. **Falcora operates where the work is hardest: Detect & Respond.**

| Govern | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| Organizational Context | Asset Management | Identity, Authentication & Access Control | Adverse Event Analysis | Incident Management | Recovery Plan Execution |
| Risk Management Strategy | Risk Assessment | Awareness & Training | Continuous Monitoring | Incident Analysis | Recovery Communication |
| Roles & Responsibilities | Supply Chain Risk Management | Data Security | | Response Reporting & Communication | |
| Policies & Procedures | | Platform Security | | Incident Mitigation | |
| | | Infrastructure Resilience | | | |

Source: NIST SP 1299 · nvlpubs.nist.gov

SIEM & SOC

# The operating model of modern security monitoring.

Technology + Operations = effective security monitoring.

## SIEM — Security Information & Event Management

### The Technology Foundation

**Purpose**

Central platform for security data collection, detection, and alert generation.

+

## SOC — Security Operations Center

### The Operational Execution Layer

**Purpose**

Operational team and processes that investigate alerts and respond to security incidents.

(SAP)-Log → Event-based Pattern → Technical Alert → Qualified Alert → Evaluation → Incident

TEIL 1 · DER BLINDE FLECK SAP

# Warum SAP-SOC-Betrieb so schwierig ist.

Selbst mit guter Detection ist der tägliche SOC-Betrieb die eigentliche Herausforderung.



### Spezialwissen

Nur wenige Analysten können einen SAP-Alarm bewerten

### Compliance-Anforderungen

Erwartungen von Prüfern und Regulatorik

### Technische Komplexität

Hybride Landschaften & Log-Formate

### Business-Kontext

Jeder Alarm braucht seine SAP-Bedeutung

### Integration

SAP an SIEM- und SOC-Tools anbinden

### Kosten & Skalierung

Die Kosten wachsen mit jedem System

TEIL 2 · SICHTBARKEIT MIT FALCORA

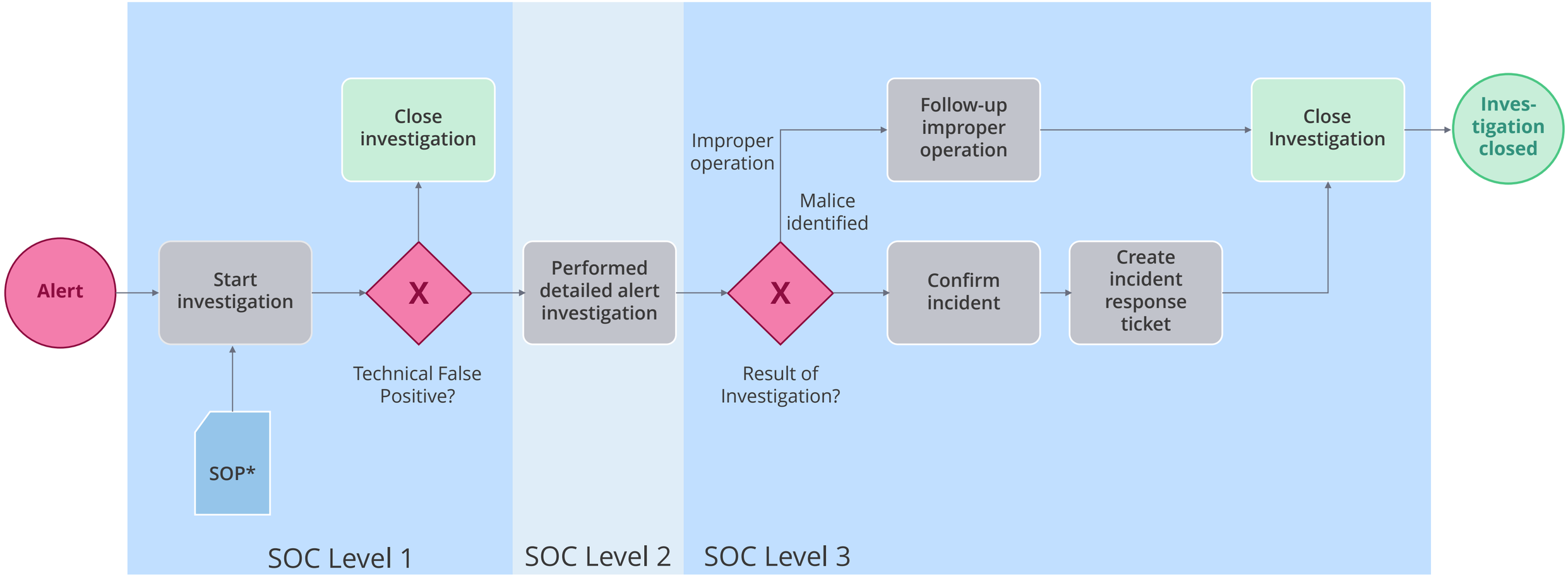
# Vom Alert zur Entscheidung.

Wie Falcora aus SAP-Logs Kontext macht – und aus Kontext eine Entscheidung.

02

Klassisch SOC Analyst Level 1-3

# E2E SAP SOC  Process

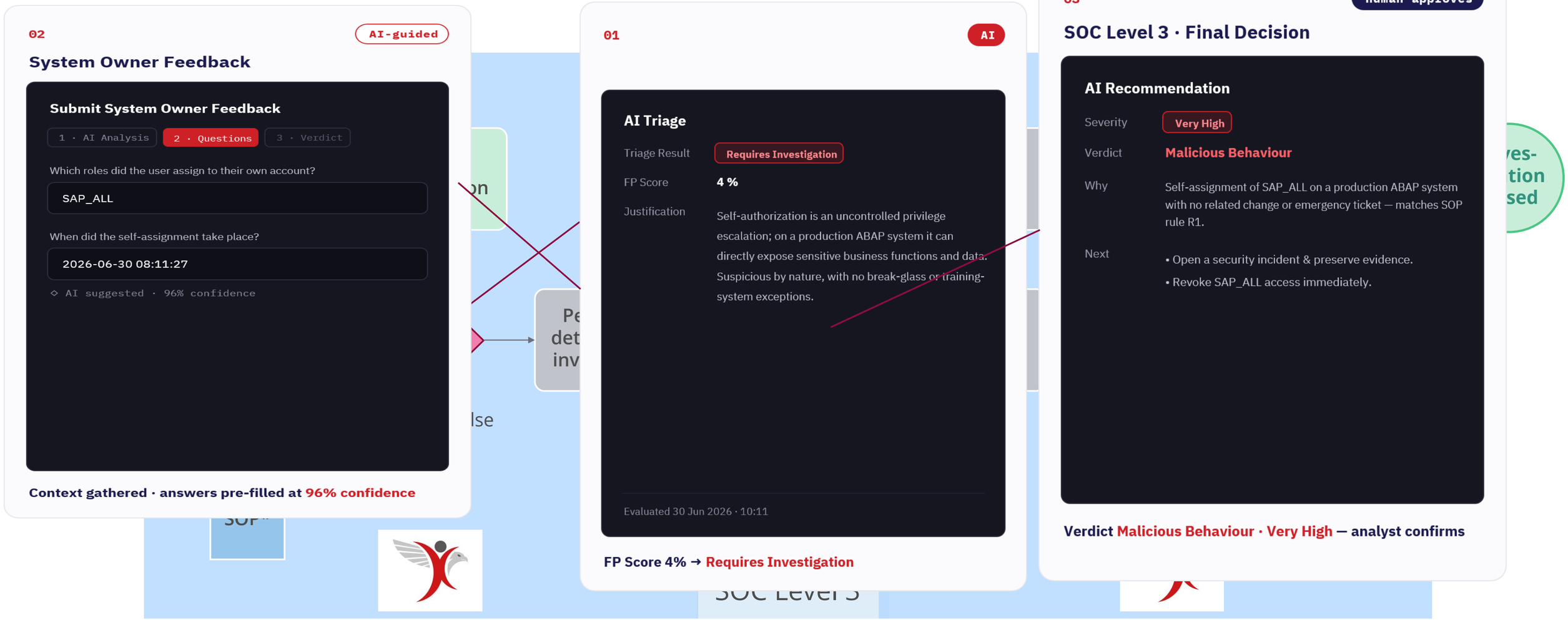



* Standard Operation Procedure

© 2026 Xiting AG. All rights reserved

New Xiting Falcora SOC Analyst

# Xiting Falcora Solution




* Standard Operation Procedure

© 2026 Xiting AG. All rights reserved

DER NÄCHSTE SCHRITT

# Und jetzt: Incident Response direkt durch die KI?

ZIEL

## Sekunden

Agent greift direkt ein

### 01 Befund steht

01 AI

**AI Triage**

| | |
|---|---|
| Triage Result | Requires Investigation |
| FP Score | 4 % |
| Justification | Self-authorization is an uncontrolled privilege |

### 02 KI-Agent

AUTONOM?

→ User sperren ?
→ SAP_ALL entziehen ?
→ Sessions beenden ?
→ Incident-Ticket anlegen ?

### 03 SOC-L3-Freigabe

03 Human approves

**SOC Level 3 · Final Decision**

**AI Recommendation**

| | |
|---|---|
| Severity | Very High |
| Verdict | Malicious Behaviour |
| Why | Self-assignment of SAP_ALL on a production ABAP system |

LEITPLANKEN

# Lesen automatisch. Eingreifen mit Freigabe.

Die Autonomie richtet sich nach der Wirkung einer Aktion – nicht nach dem technisch Möglichen.

AUTOMATISIERT DURCH DEN KI-AGENTEN

MENSCH ENTSCHEIDET

**01**
### Kontext sammeln
Rollen, Belege, Audit Log – nur lesend.

**02**
### Enrichment
Zugriff auf SAP Backend

**03**
### Bewerten & empfehlen
Wie kritisch? Was ist zu tun?

**04**
### Freigabe
User sperren – ja oder nein?

**05**
### Ausführen & belegen
Sperren und jeden Schritt belegen.

Enrichment

# Was braucht der Agent?

Dieselben Standard-BAPIs wie in der Benutzerverwaltung – nach Freigabe, mit eigenem technischen User.

XITING FALCORA DIRECT

## KI-Response-Agent

- **Liest den Vorfall** · Alert, Kontext, Risiko
- **Wählt den Playbook-Schritt** · innerhalb der Leitplanken
- **Führt aus & dokumentiert** · Freigabe, wo nötig

**Enrichment**

`z.B. BAPI_USER_GET_DETAIL`

→

## SAP Cloud Connector

Outbound-Tunnel aus dem Kundennetz, mit Allow-List je System.

BAPI · FM

→

techn. User

BACKEND · ABAP-SYSTEME

- **S/4HANA** · on-prem, private
- **SAP ECC**
- **BW · GRC · Solution Manager**

LEITPLANKEN

# Lesen automatisch. Eingreifen mit Freigabe.

Die Autonomie richtet sich nach der Wirkung einer Aktion – nicht nach dem technisch Möglichen.

AUTOMATISIERT DURCH DEN KI-AGENTEN

MENSCH ENTSCHEIDET

**01**
### Kontext sammeln
Rollen, Belege, Audit Log – nur lesend.

**02**
### Enrichment
Zugriff auf SAP Backend

**03**
### Bewerten & empfehlen
Wie kritisch? Was ist zu tun?

**04**
### Freigabe
User sperren – ja oder nein?

**05**
### Ausführen & belegen
Sperren und jeden Schritt belegen.

## BERECHTIGUNG DES AGENTEN

Einmal je System eingerichtet, mit SAP-Standardmitteln.

- **Getrennte technische User**
- **S_RFC nur für freigegebene Bausteine**
- **Allow-List im SAP Cloud Connector**

## NACHVOLLZIEHBARKEIT & KONTROLLE

Jeder Schritt muss protokolliert werden

- **Audit Trail je Case**
- **Freigabestufen vorab vereinbart**
- **Klare Zuordnung**

TEIL 3 · PRAXISBEISPIEL

# Ein Alert in Falcora – vom Log bis zur Eindämmung.

**Selbstzuweisung von Berechtigungen in Produktion – Schritt für Schritt in Falcora, mit Fortinet-Kontext.**

03

FALCORA – DIE PLATTFORM

# Jede SAP-Security-Entscheidung – voll informiert.

Falcora liefert jede Information, die eine SAP-Security-Entscheidung braucht.



01

## Operations

Erkennt verdächtige SAP-Aktivitäten und erklärt sie verständlich – rund um die Uhr.

02

## Automatic Response

Klärt Rückfragen selbst und sperrt nach Freigabe direkt im SAP-System.

03

## Security Notes

Zeigt, welche SAP-Hinweise in Ihrer Landschaft wirklich dringend sind.

04

## Forensics

Beantwortet Prüferfragen über alle Systeme – auch Monate zurück.

**— KI erledigt die Arbeit. Der Mensch trifft die Entscheidung.**

DER USE CASE

# Der Ausgangspunkt: Ein User berechtigt sich selbst.

Ein bekannter Fall – Falcora bewertet ihn mit hinterlegtem SAP-Wissen statt zu raten.

IN DER WISSENSBASIS

- **Detection-Content & Use Cases**
- **Risikoerhöhende Indikatoren**
- **Alert-Muster**
- **Fragen an den System Owner**
- **SOP-Bewertungsregeln**
- **Remediation & Response**

USE CASE · AUTHZ.2.1

## Zuweisung von Berechtigungen an den eigenen User

| | |
|---|---|
| MUSTER | Ein User weist seinem eigenen Konto Berechtigungen zu. |
| RISIKO | Kritische Berechtigung (SAP_ALL) · Produktivsystem · kein Change-Ticket. |
| SOP-REGELN | R1 Böswillig · R2 Fehlbedienung · R3 Notfallzugriff · R4 Offene Lücken. |
| OWNER-FRAGEN | Welche Rollen? Wann? Wer hat es ermöglicht? |
| REMEDIATION | Zugriff entziehen · Beweise sichern · Folgeaktivität prüfen. |

Einer von hunderten kuratierten Use Cases

SO NUTZT FALCORA DIE WISSENSBASIS · RAG

01 · RETRIEVAL
**Vektordatenbank**
Findet passende Use Cases und SOP-Regeln.

►

02 · GENERATION
**LLM**
Bewertet den Alert im SAP-Kontext.

►

03 · ERGEBNIS
**Empfehlung**
Urteil, FP-Score und Begründung.

SCHRITT 1 · ERKENNEN

# Drei Alarme. Ein User. Ein Vorfall.

Falcora lernt das normale Verhalten je User – und fasst Abweichungen zu einer Geschichte zusammen.

USER JDOE · PRODUKTION

**02:14** — **Weist sich SAP_ALL zu**

**02:19** — **Liest sensible Tabellen**
Gehalts- und Lieferanten-Bankdaten – nie zuvor genutzt.

**02:26** — **Lädt eine kritische Datei**
Export auf den lokalen Rechner.

FALCORA · VERHALTENSANALYSE

## Ein zusammenhängender Vorfall

Rechte holen → Daten ansehen → Daten mitnehmen. Zwölf Minuten, ein Konto.

- **Normalverhalten je User** · Rollen, Tabellen, Uhrzeiten
- **Alarme verknüpft** · über Systeme hinweg
- **Risiko steigt** · mit jedem Schritt

**1 kritischer Vorfall – statt 3 einzelner Tickets**

SCHRITT 2 · VERKNÜPFEN MIT FORTINET

# SAP und Netzwerk – endlich ein gemeinsames Bild

Falcora sieht, was in SAP passiert. Fortinet sieht, woher der Zugriff kam.

FORTINET

**SAP-LANDSCHAFT**

- S/4HANA, ECC
- SAP BTP
- SuccessFactors
- RFC & Gateway

→ ←

**XITING FALCORA**

## SAP-Kontext & KI-Agent

- Erkennen
- Bewerten
- Empfehlen
- Belegen

→ ←

**FORTINET · NETZSICHT**

### FortiAnalyzer · FortiSIEM

VPN-Anmeldung, Netzangriffe, Zustand des Rechners.

→

**FORTINET · REAKTION**

### FortiSOAR · FortiGate

IP sperren, VPN trennen – nach Freigabe.

### 01 · Erkennen

User gibt sich SAP_ALL – in Produktion, ohne Change.

### 02 · Verknüpfen

Zugriff kam per VPN von einem auffälligen Rechner.

### 03 · Bewerten

Hohes Risiko, klare Empfehlung.

### 04 · Eindämmen

User sperren, IP blocken – nach Freigabe.

ITing quality

TAKEAWAYS

# Vier Dinge zum Mitnehmen

Sichtbarkeit entsteht nicht durch mehr Logs, sondern durch Kontext.

ZUM MITNEHMEN

**01** **Mehr Autonomie heißt auch mehr Komplexität**

Ein Owner je Agent, eigene technische User mit Least Privilege.

**02** **Jede Agent-Aktion belegbar machen**

Lesen automatisch, eingreifen nur mit Freigabe – alles protokolliert.

**03** **Protect braucht Detect**

Berechtigungen schützen nur, wenn jemand ihre Umgehung sieht.

**04** **Kontext schlägt Menge**

SAP-Kontext plus Netz-Telemetrie: weniger Alerts, klarere Entscheidungen.

DIE ROLLE DES MENSCHEN

**Falcora übernimmt die Ermittlung. Der Mensch trifft die Entscheidung.**

Und bleibt dafür verantwortlich – das ist kein Mangel, sondern Design.



# It’s time to fall in love with SAP logs




*Because they tell you everything — if you understand them*

© 2026 Xiting AG. All rights reserved

# Q & A



# Vielen Dank
# für Ihre Aufmerksamkeit!


**Moritz Holeschovsky**
Head of SAP Cybersecurity & Security Monitoring

**E-Mail:** mholeschovsky@xiting.com

**Xiting GmbH**

Obere Ringstraße 17
79859 Schluchsee

**E-Mail:** info@xiting.com
**Web:** www.xiting.com


**Hier vernetzen**

Wenn Sie weitere Informationen benötigen, können Sie mich gerne kontaktieren.