FORTINET

SAP trifft Infrastruktur

Smartere Security Operations

Julian Petersohn (jpetersohn@fortinet.com)

Ein Dienstagabend, 21:30 Uhr

Sechs Ereignisse in 40 Minuten - verteilt auf mehrere Teams und Konsolen



01

Helpdesk

21:30 · Identität

02

VPN-Login

21:47 · Netz

03

Port-Scan

21:52 · Netz

04

RFC-Logon

21:58 · SAP

05

SE38-Report

22:03 · SAP

06

Upload

22:09 · Netz

Jedes Signal allein ist erklärbar - zusammen ist es ein Angriff

© Fortinet Inc. All Rights Reserved.

Zwei Teams, zwei Konsolen, ein Vorfall

SAP Security und SOC sehen jeweils nur die Hälfte

SAP Security sieht

Benutzer, Rolle, Berechtigung, Transaktion

Security Audit Log, RFC-Aufrufe, Änderungsbelege

Aber nicht: woher die Verbindung kam - und ob das Endgerät kompromittiert ist

Das SOC sieht

IP, Gerät, VPN-Session, Firewall-Policy

IPS-, Malware- und Botnet-Treffer, Datenvolumen

Aber nicht: was SE38 oder S_RFC bedeutet - und ob der User kritisch berechtigt ist

© Fortinet Inc. All Rights Reserved.

Warum jetzt: ein kritischer Exploit im SAP-Kernel

CVE-2026-44756 im SAP Kernel (ABAP & Java)

08. September 2026

CVSS 10.0 - „OVERPASS“ (Onapsis) - unabhängige Forscher erreichten im Labor in ca. 48 h einen funktionierenden RCE



Memory Corruption bei der Verarbeitung des SAP Extended Passport (EPP)

Betroffen sind DIAG, RFC, WebSocket-RFC und HTTP - also genau die Wege, über die SAP erreichbar ist. Exposure-Reduktion und geprüfte kompensierende Kontrollen verkleinern die Angriffsfläche drastisch. SAP-Patching und Compromise Assessment bleiben Pflicht.

© Fortinet Inc. All Rights Reserved.

Das Prinzip: drei Bausteine, ein Ablauf

SAP-Kontext und Infrastruktur-Telemetrie münden in eine gesteuerte Reaktion



SAP-Kontext

Xiting Falcora

Wer, was, mit welcher Berechtigung - wie kritisch?



Infrastruktur-Telemetrie

FortiAnalyzer, FortiSIEM

Woher, welches Gerät, welche Threats?



Gesteuerte Reaktion

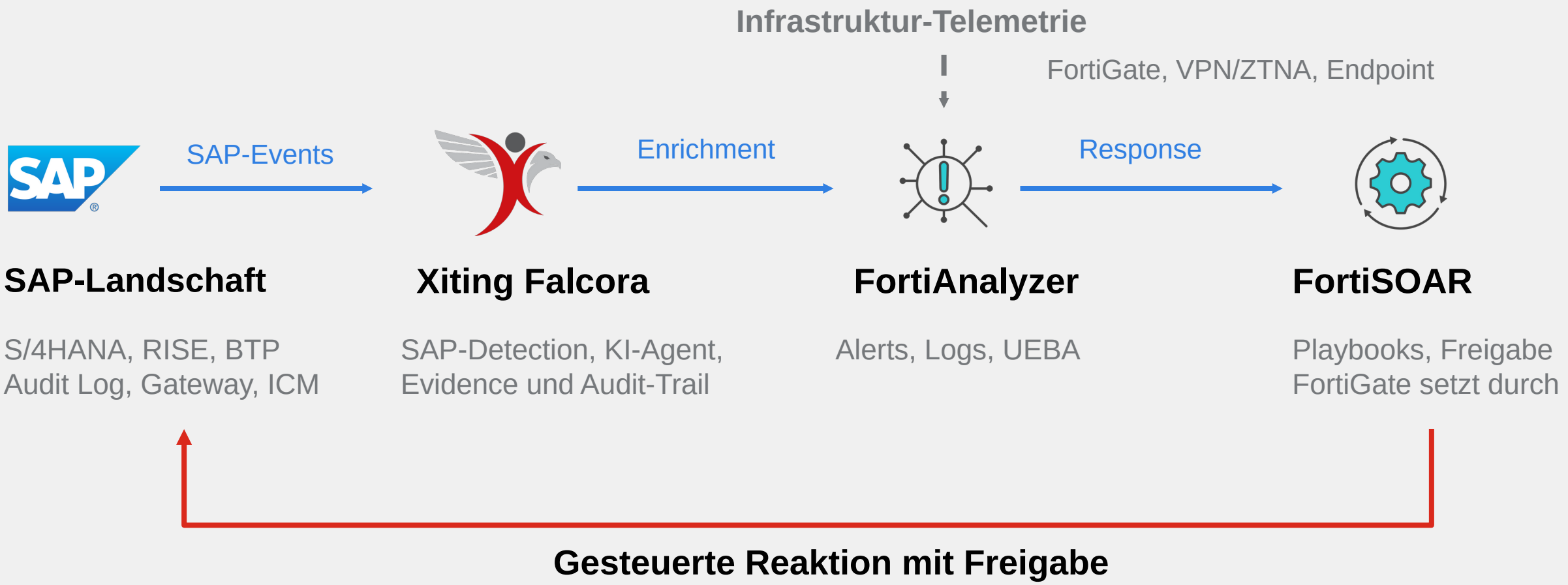
FortiSOAR, FortiGate

Sperren, isolieren, blocken - mit klarer Freigabe.

© Fortinet Inc. All Rights Reserved.

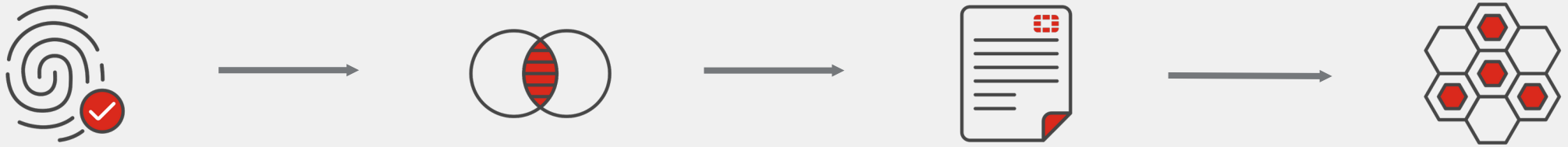
Architektur: Xiting Falcora trifft Fortinet Security Fabric

SAP-Kontext von Xiting, Infrastruktur-Kontext und Durchsetzung von Fortinet



© Fortinet Inc. All Rights Reserved.

Use Case: ein Alert, angereichert in einem Durchlauf



Erkennen

Falcora: RFC-Logon techn. User auf PRD

Korrelieren

SAP: kritische Rollen
FAZ: VPN, IPS, UEBA

Bewerten

KI-Agent bewertet: Risiko hoch

Eindämmen

Sperren, blocken - nach Freigabe

Lesende Enrichment-Actions, Zeitfenster ±15 min um das SAP-Event

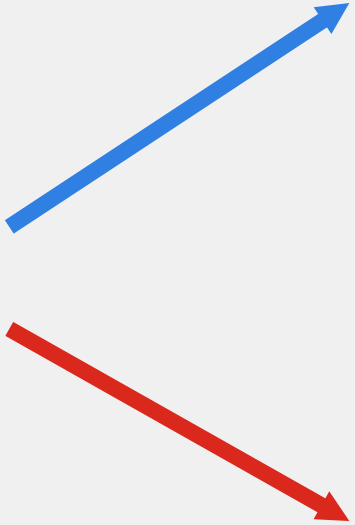
© Fortinet Inc. All Rights Reserved.

Automatisieren, was sicher ist - freigeben, was wehtut

Evidence automatisch sammeln, eingreifende Aktionen gesteuert ausführen

FortiSOAR

Angereicherter SAP-Incident



Automatisch

Evidence aus SAP, FortiAnalyzer und FortiSIEM sammeln, Ticket anlegen

Mit Freigabe

IP blocken, Session beenden (SOC), SAP-User sperren (System Owner)

© Fortinet Inc. All Rights Reserved.

Stark im Verbund: Xiting, Accenture, Fortinet

Falcora: AI-native Detection und Response für SAP

Berechtigungen, IAM, Access Governance

Tiefe SAP-Expertise aus Projekten

SAP-Security-Strategie und Programme

Integration in großen, hybriden Landschaften

Prozesse, Organisation und Betrieb

Telemetrie: FortiAnalyzer, FortiSIEM

Durchsetzung: FortiGate, ZTNA, SD-WAN

Orchestrierung: FortiSOAR

© Fortinet Inc. All Rights Reserved.

Klein starten, messbar wachsen

1 Baseline schaffen

Kritische SAP-Systeme und Owner kennen

Zugriffswege und Log-Lücken finden

Einen Use Case priorisieren

2 Lesend pilotieren

Enrichment für zwei bis drei Use Cases

Etwa RFC-Missbrauch, Dienstleister-Zugriff

MTTA und MTTR vorher und nachher messen

3 Gesteuert ausbauen

Response-Playbooks mit Freigabestufen

SOC und SAP Basis an einen Tisch

Weitere Systeme und Signale anbinden

© Fortinet Inc. All Rights Reserved.

Drei Dinge zum Mitnehmen



Über SAP hinausdenken

SAP-Sicherheit endet nicht im SAP-System - Angriffe kommen über Netz, Endgeräte und Dienstleister.



Kontext schlägt Volumen

Weniger Alerts - dafür solche, über die man entscheiden kann.



Automatisieren mit Leitplanken

Lesen automatisch, eingreifen mit Freigabe.

© Fortinet Inc. All Rights Reserved.


FORTINET