Moderne KI-Lösungen in PAM:
Revolution für die privilegierte Zugriffskontrolle

FUDO SECURITY

Stefan Rabben

Regional Director DACH

M: +49 162 283 69 73
E: s.rabben@fudosecurity.com

Agenda

- Die Ausgangslage
- Die Konsequenz
- Die Aufgabe von Privileged Access Management (PAM)
- Die Basisarchitektur
- Die Herausforderung
- **Einsatz von KI**
- **Analyse durch KI**
- **Training der KI**
- Bedeutung für die Compliance
- Best Practises
- Warum Fudo Security?

Die Ausgangslage

53,8% der erfolgreichen Cyberangriffe

basieren auf unautorisiertem Netzwerkzugriff

Quelle: BlackKite 3rd-Party-Report für 2024

33% der erfolgreichen Cyberangriffe

hängen mit privilegierten Nutzern zusammen.

Quelle: Forrester-Report für 2021: Cybersicherheit

27% der erfolgreichen Cyberangriffe

basieren auf Ransomware

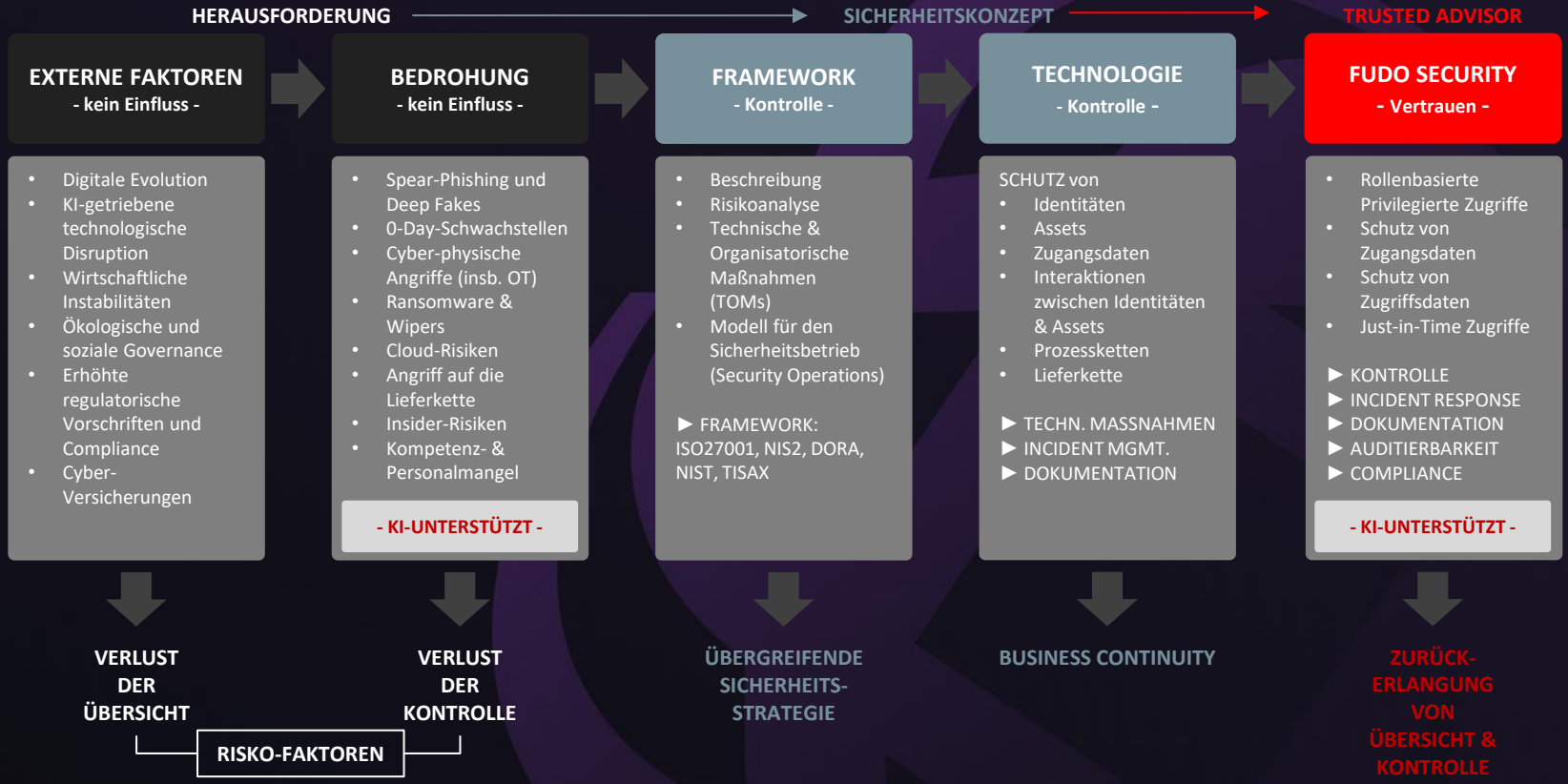
Quelle: BlackKite 3rd-Party-Report für 2023

40% der erfolgreichen Cyberangriffe

wurden durch gestohlene Anmeldeinformationen verursacht.

Quelle: Verizon Datenleck-Report 2022

Die Ausgangslage



Die Konsequenz

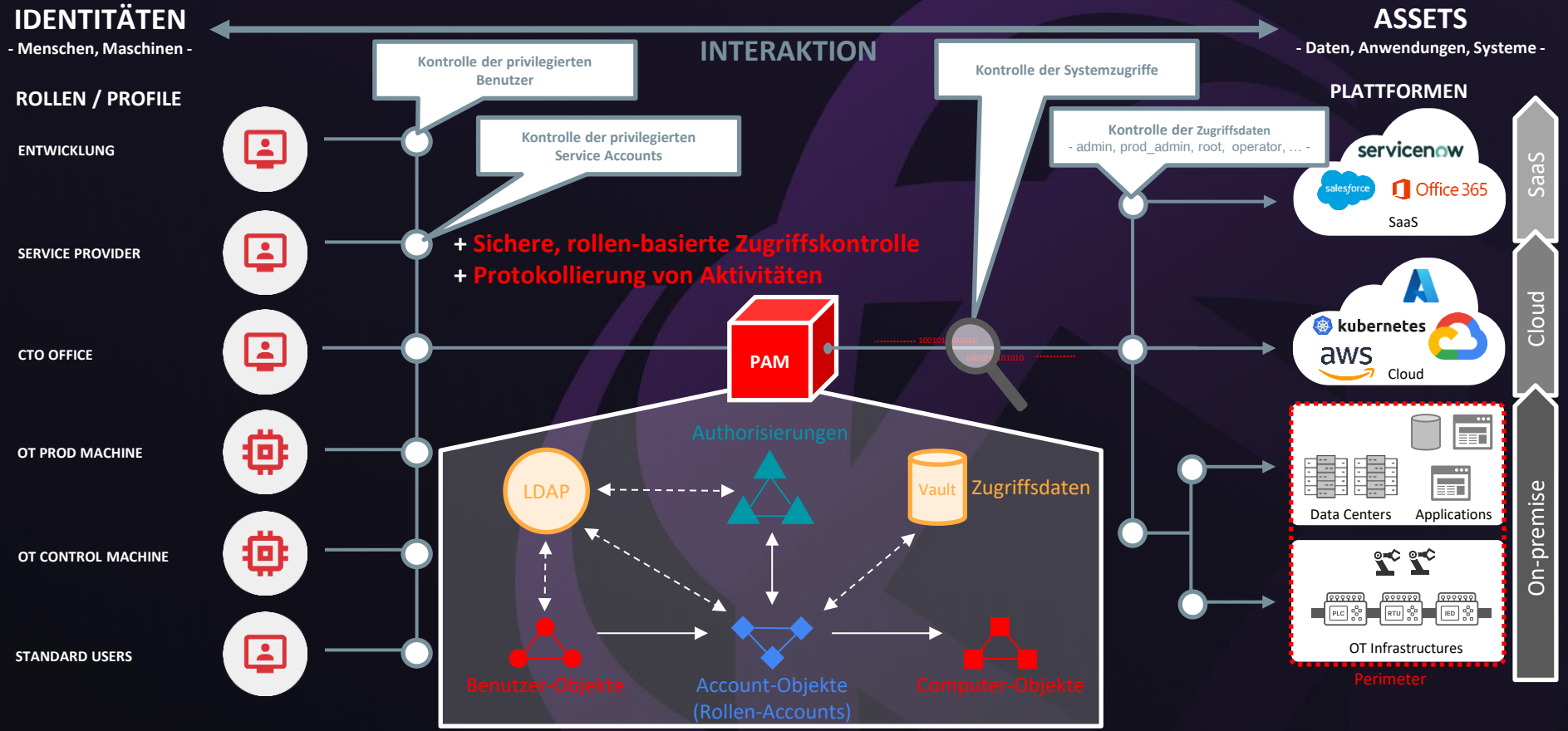
Kontrolle der Systemzugriffe

Kontrolle der privilegierten Benutzer

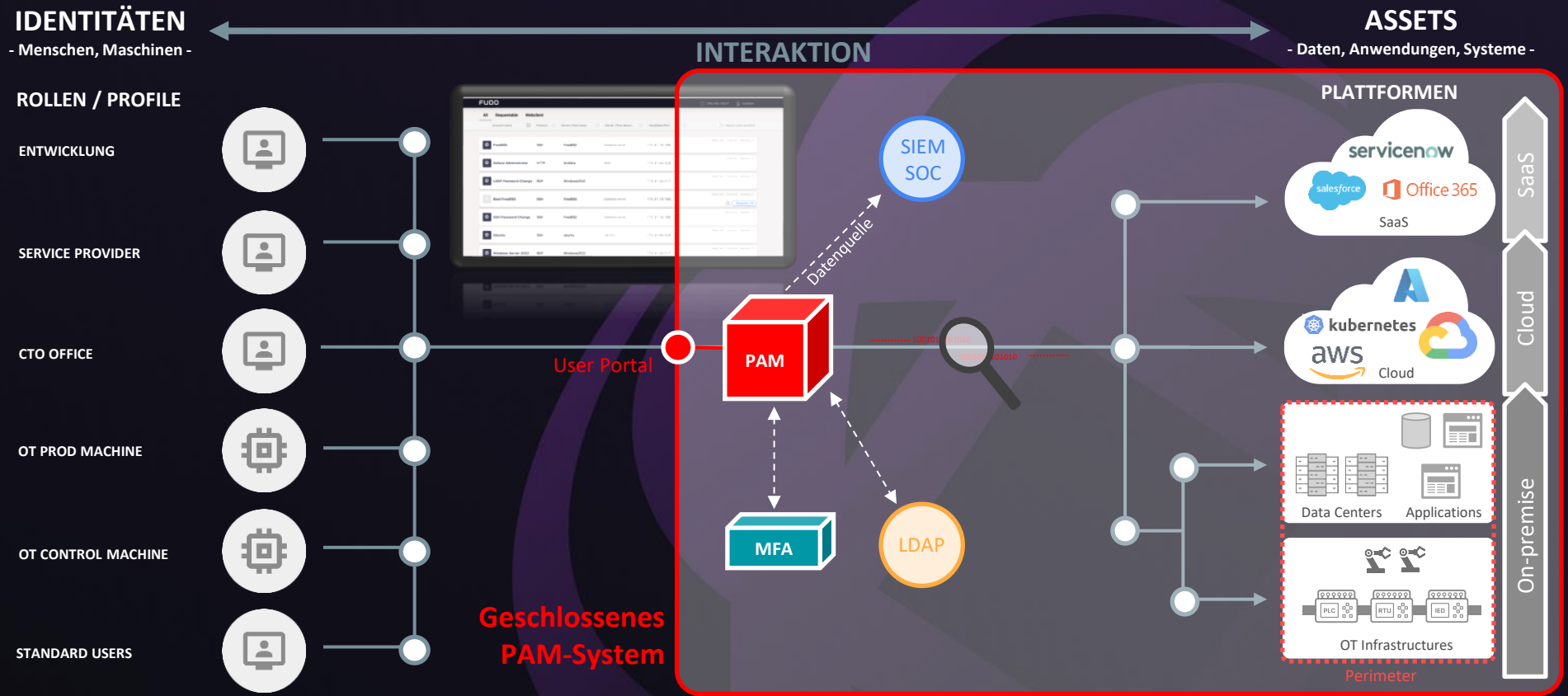
Kontrolle privilegierter Service Accounts

Kontrolle der Zugriffsdaten

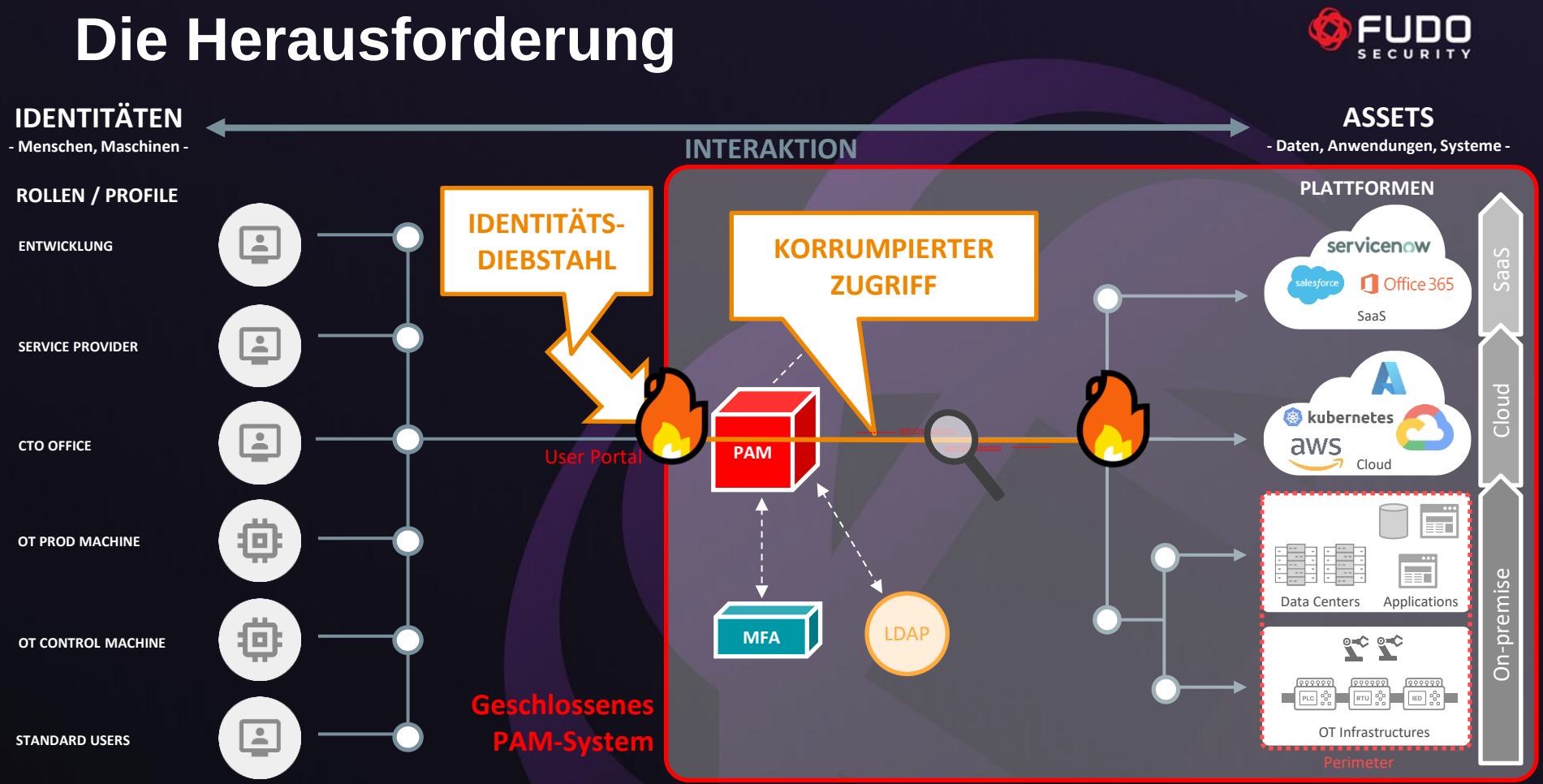
Die Aufgabe von PAM



Die Basisarchitektur von FUDO PAM



Die Herausforderung

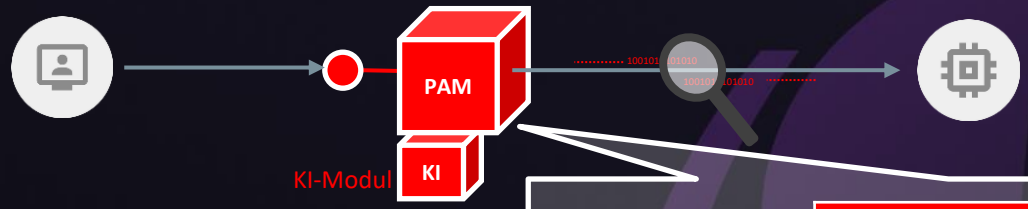


Der Einsatz von KI

PAM überwacht privilegierte Sitzungen

Benutzerverhalten

Integriertes KI-Modul analysiert Benutzerverhalten

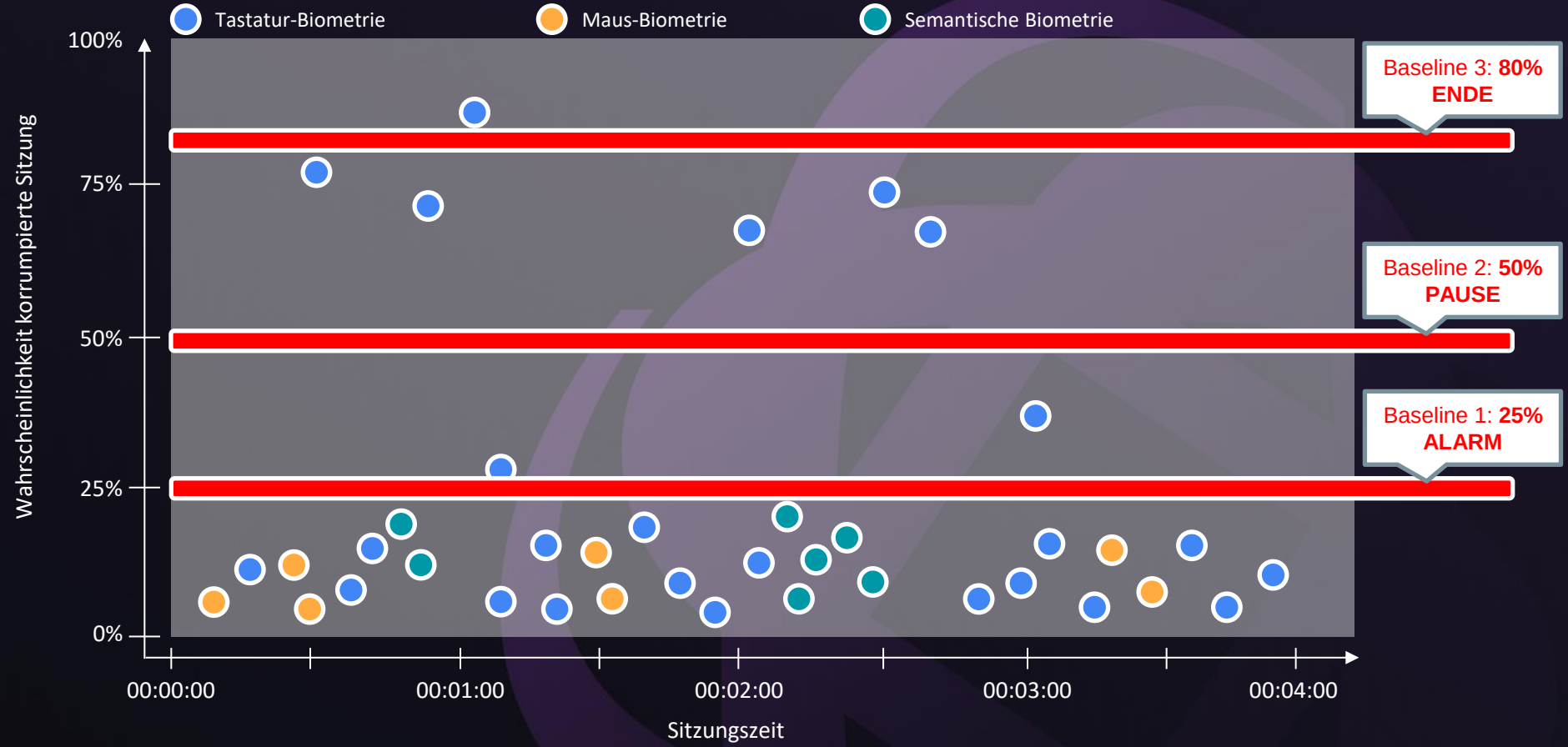


Benutzer-Objekte

Objekteigenschaft: Verhaltensprofil

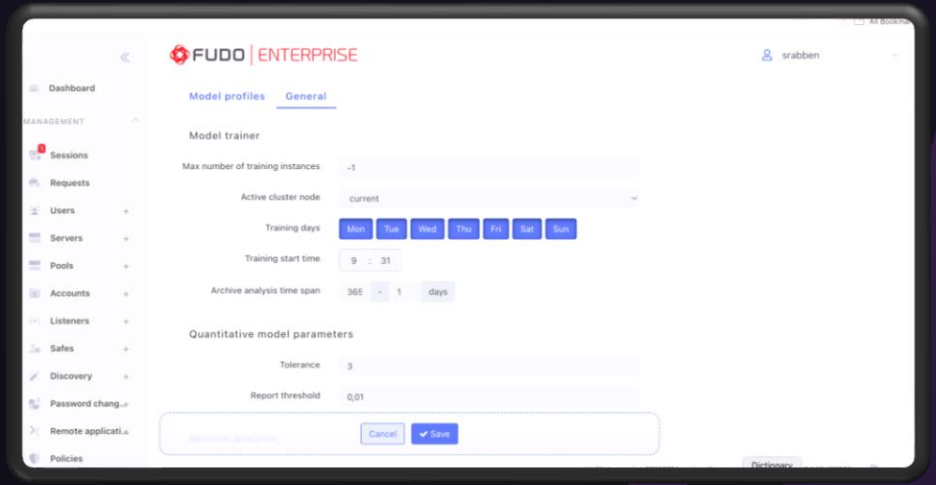
Biometrie	Trainingsgrad
Tastatur-Biometrie	75%
Maus-Biometrie	50%
Semantische Biometrie	80%

Analyse durch KI

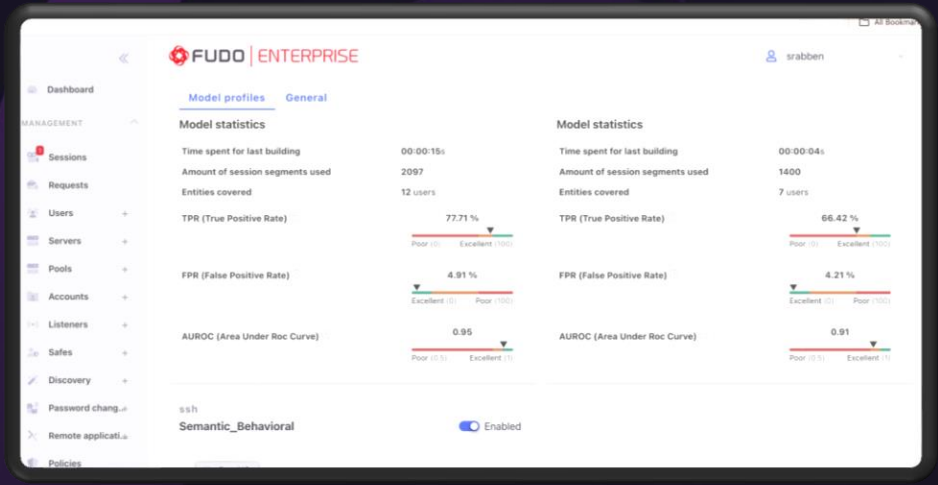


Training der KI

KI-Modell Trainer



KI-Modell Statistiken

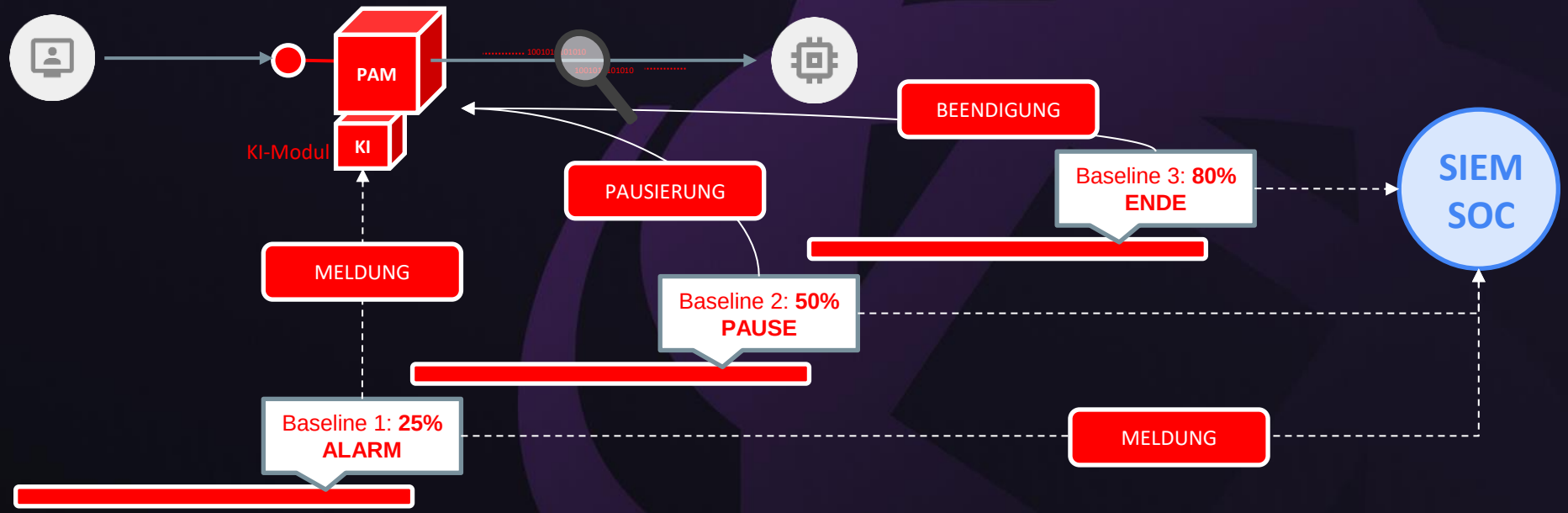


Incident Management durch KI

PAM überwacht privilegierte Sitzungen

Benutzerverhalten

Integriertes KI-Modul analysiert Benutzerverhalten



Bedeutung für die Compliance

hier: NIS2

Präambel	Beschreibung der Zielsetzungen	144 Absätze
Kapitel I	Allgemeine Bestimmungen	Artikel 1 - 6
Kapitel II	Koordinierte Rahmen für die Cybersicherheit	Artikel 7 - 13
Kapitel III	Zusammenarbeit auf Unions- und internationaler Ebene	Artikel 14 - 19
Kapitel IV	Risikomaßnahmen im Bereich der Cybersicherheit	Artikel 20 - 25
Kapitel V	Zuständigkeit und Registrierung	Artikel 26 - 28
Kapitel VI	Informationsaustausch	Artikel 29 - 30
Kapitel VII	Allgemeine Aspekte der Aufsicht und Durchsetzung	Artikel 31 - 37
Kapitel VIII	Delegierte Rechtsakte und Durchführungsrechtsakte	Artikel 38 - 39
Kapitel IX	Schlussbestimmungen	Artikel 40 - 46

Zielsetzung

- 33: Fernzugriff auf Cloud-Dienste
- 49: Cyberhygiene von Verfahren
- 51: Innovative Technologien
- 57: Aktiver Cyberschutz
- 83: Sicherheit von Tätigkeiten
- 89: Cyberhygiene von Infrastruktur
- 98: Verschlüsselung
- 102: Incident Management

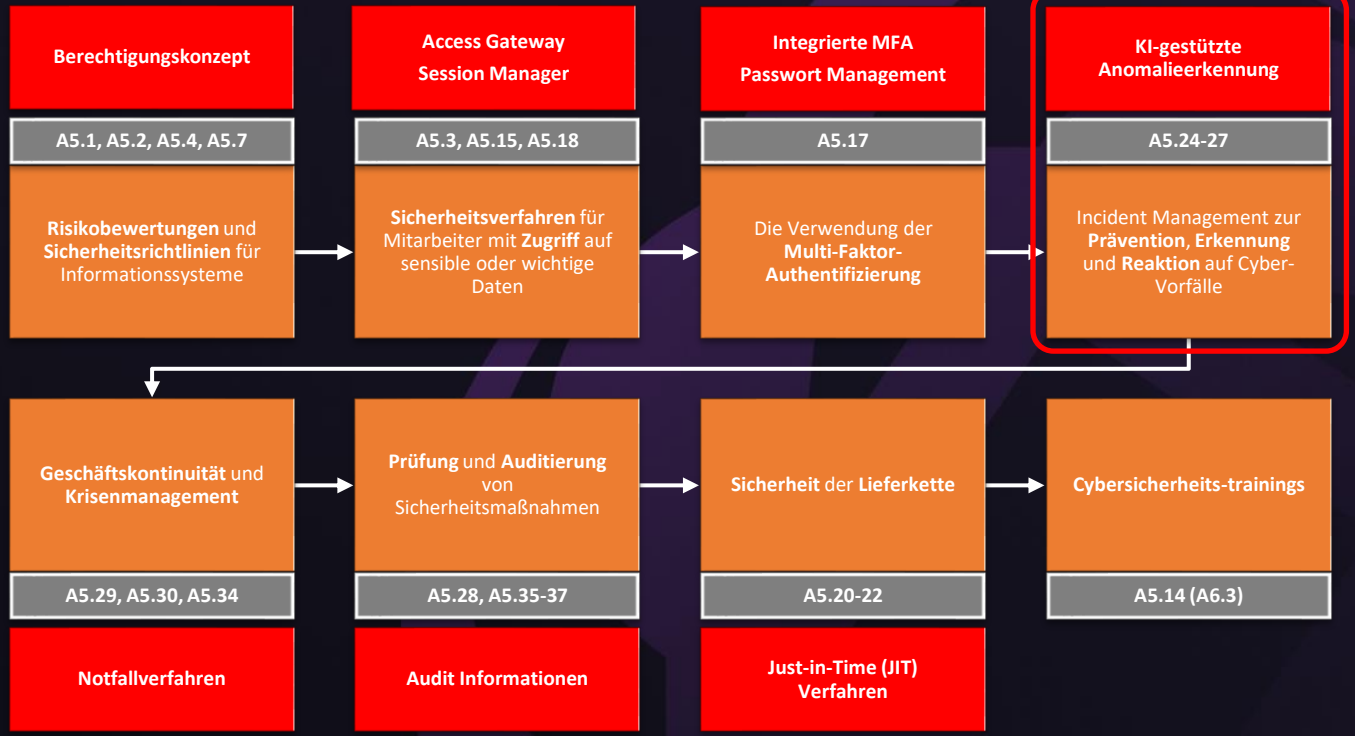
Umsetzung

- 21: Risiko Mgmt Maßnahmen

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

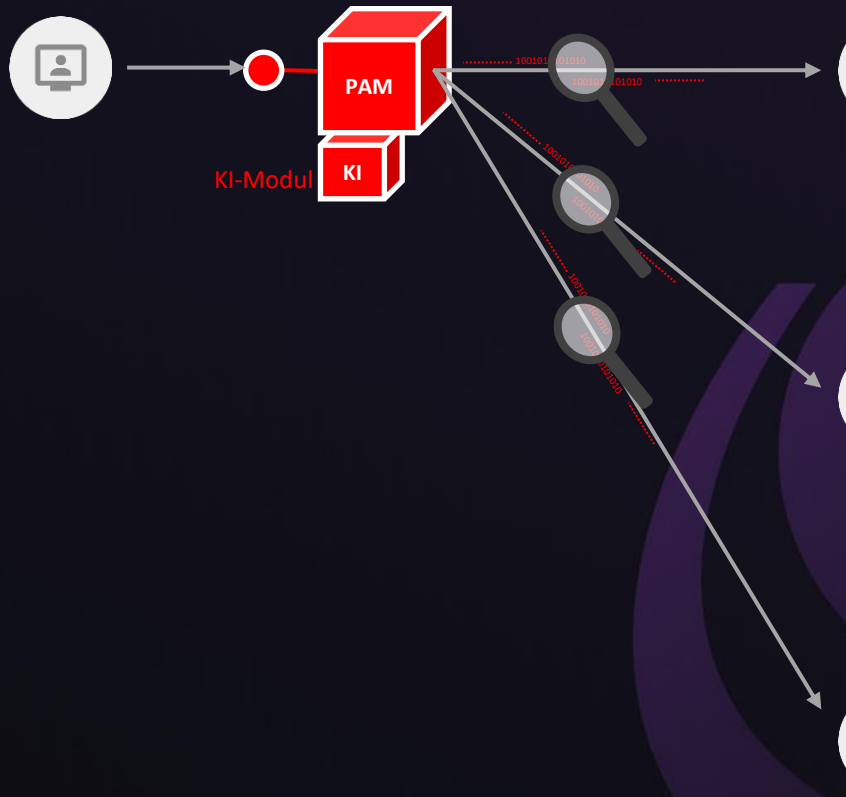
Risikomanagement-Maßnahmen

nach Kapitel IV, Artikel 21, NIS2



ISO27001:2022 A5

Best Practises



RISK 0 SYSTEME
- SEHR HOHES RISIKO -

Zugriff auschließlich über PAM
- Genehmigungsworkflow (4-Augen)
- Multi-Faktor Authentifizierung
- Videoüberwachung
- Passwort-Rotation: alle 120 min

RISK 1 SYSTEME
- HOHES RISIKO -

Zugriff auschließlich über PAM
- Genehmigungsworkflow (4-Augen)
- Multi-Faktor Authentifizierung
- Videoüberwachung
- Passwort-Rotation: wöchentlich

RISK 2 SYSTEME
- MITTLERES RISIKO -

Privilegierter Zugriff über PAM
- Genehmigungsworkflow (2-Augen)
- Multi-Faktor Authentifizierung
- Videoüberwachung für Externe
- Passwort-Rotation: monatlich

BSI-Standard: 200-2

Warum Fudo?

GLOBEE AWARDS BRONZE WINNER 2024

Bestes SM

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

NEXT GEN PRIVILEGED ACCESS MANAGEMENT

FUDO SECURITY

24 Stunden

Inbetriebnahme innerhalb von 24 Stunden

Session Management

Bestbewertetes Session Management

Beste KI

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

Innovation

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

MADE IN EUROPE

NATO-Sicherheitszertifikat

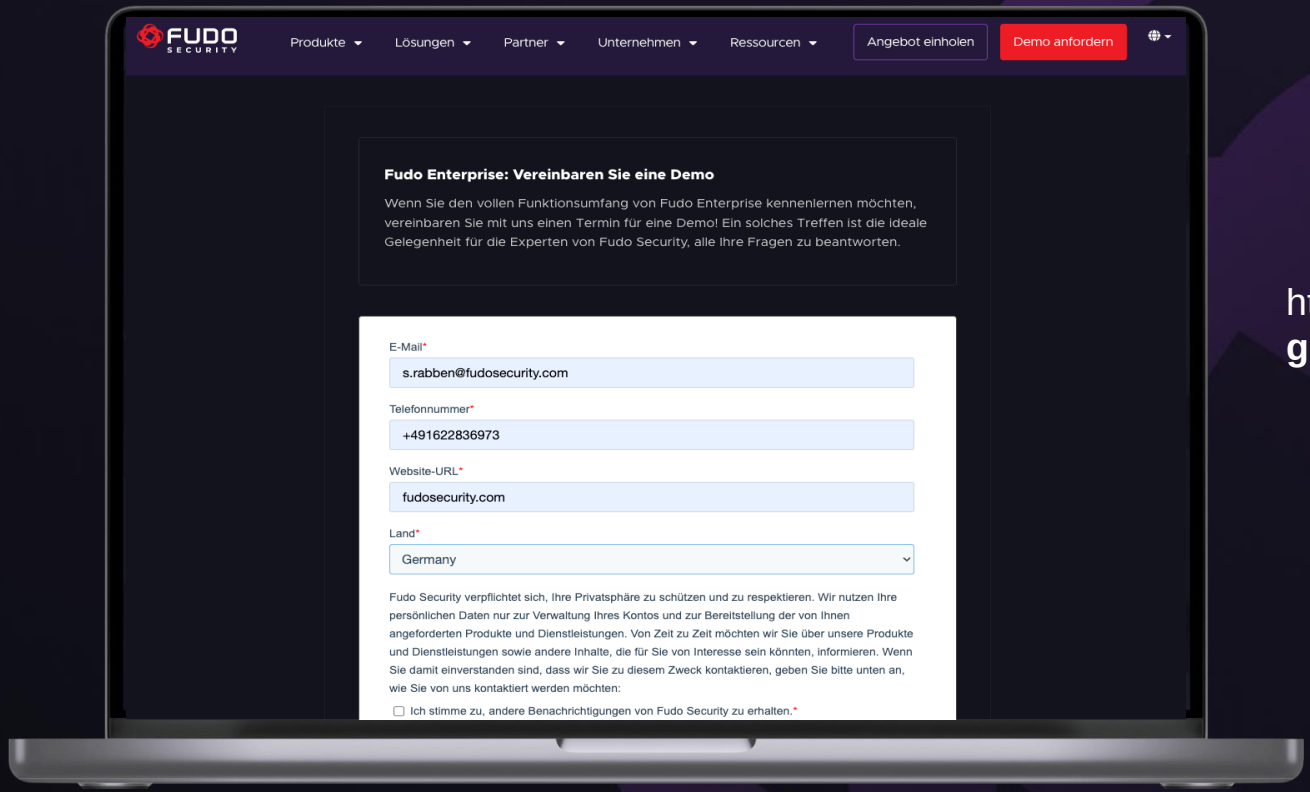
KI

Bestbewertete KI zur Anomalieerkennung & -abwehr

Sicherheitsarchitektur

Eines der sichersten PAM-Architekturen am Markt
- FreeBSD Unix als gehärtetes Betriebssystem -

Sehen Sie sich eine Demo an!



https://fudosecurity.com/de/**get-a-demo/**

Kontaktieren Sie mich!

Stefan Rabben
Regional Director DACH

M: +49 162 283 69 73
E: s.rabben@fudosecurity.com

Fudo Security Fudo Security @FudoSecurity