CONET Webinar

Identity Threat Detection and Response

04.07.2024 | Jörg Meuser

Einführung:

Agenda

Teil 01 ITDR - Einführung

Teil 02 Konzepte & Lösungen

Teil 03 Trends & Perspektiven

Teil 1

ITDR - Einführung

1

Übersicht

- EDR
- MDR
- NDR
- TDR
- XDR
- (X)DR

Bedrohungen

- Privilege Escalation
- Lateral Movement
- Credential Harvesting
- Password Spraying
- Kerberoasting
- Identity Theft

Ziele

- Schutz der Identität
- Schutz von IDM-Systemen
- Schutz von Zero Trust Umgebungen
- Proaktive Erkennung von Cyberbedrohungen
- Automatisierte Reaktion

Einsatzgebiete

- On Premise
- Client
- Cloud
- Hybride Cloud Szenarien
- Netzwerk

Teil 2

Konzepte und Lösungen

2

ITDR ist…

- **UseCase**
- **Konzept**
- **Prozess**
- **Lösung**

Typische Merkmale

- Sensoren
- Signal Verarbeitung
- Riskmonitoring / Scoring
- Echtzeit-Analyse
- Echtzeit-Reaktion

Thread Detection

- Identitäts-Kontext
- User Behavior Analytics (UBA)
- User and Entity Behavior Analytics (UEBA)
- Privileged User Behavior Analytics (PUBA)

User Behavior

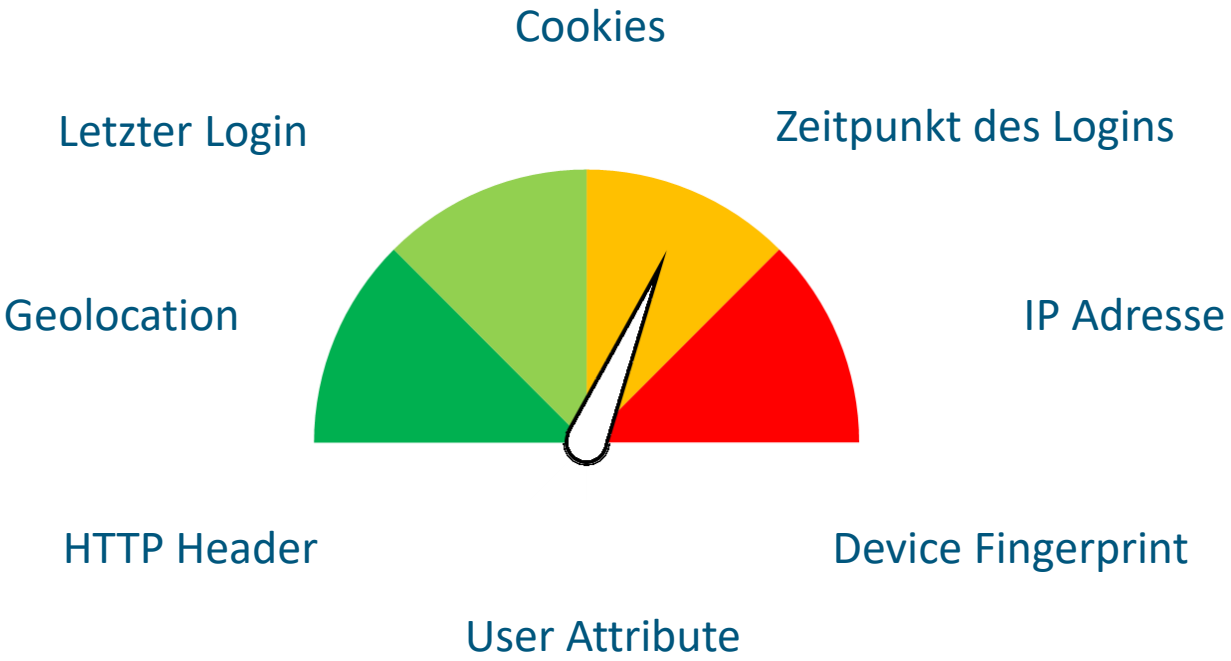
- Authentifizierung (und Fehlversuche)
- Zugriffe
- Insbesondere auf Neue Systeme/Daten
- Zuordnung Identität/Accounts
- Neue Clients und Standorte
- Zeiten und Aktivitäten

ITDR und KI

- UBA Baseline
- Maschinelles Lernen
- Künstlicher Intelligenz (KI)
- Threat LLMs
- ITDR-Systeme in Wechselwirkung mit weiteren KI-Systemen

Kontext Authentifizierung

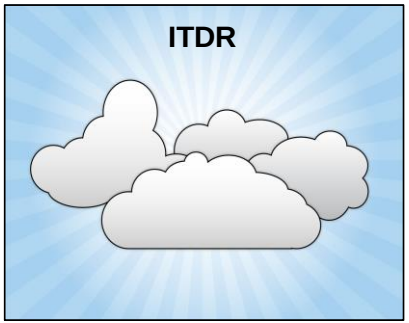
- Vor- / Zwischenevaluierung des Risikos eines Authentifizierungsversuchs auf Basis vordefinierter Faktoren



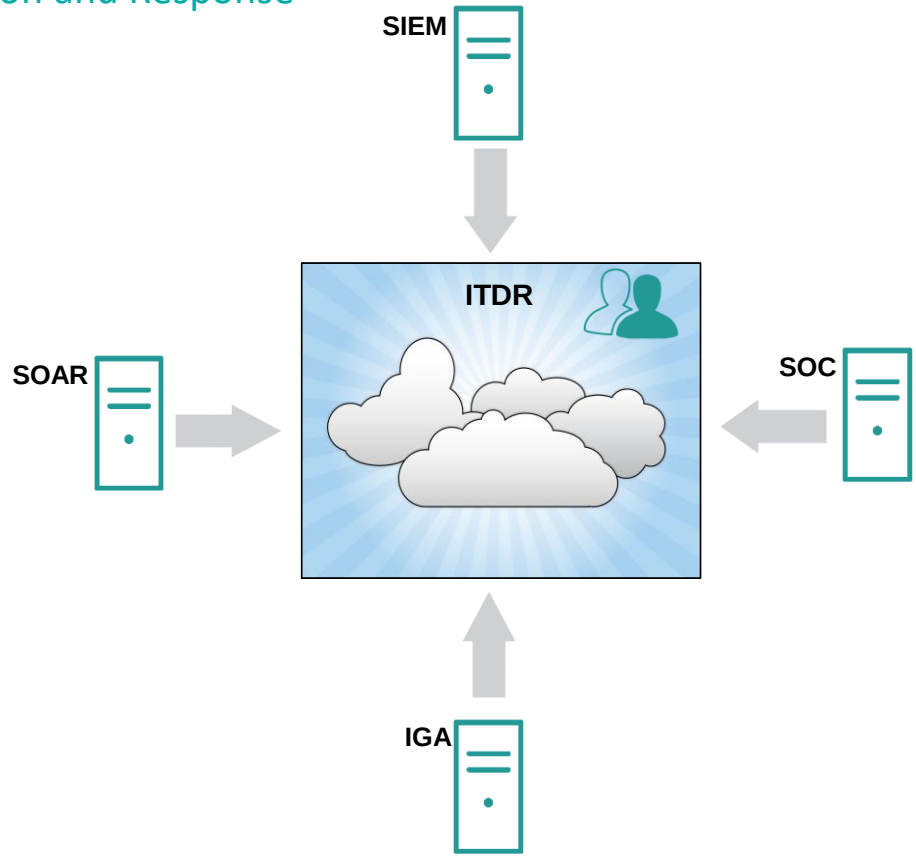
Geo-Location

Geo-Velocity

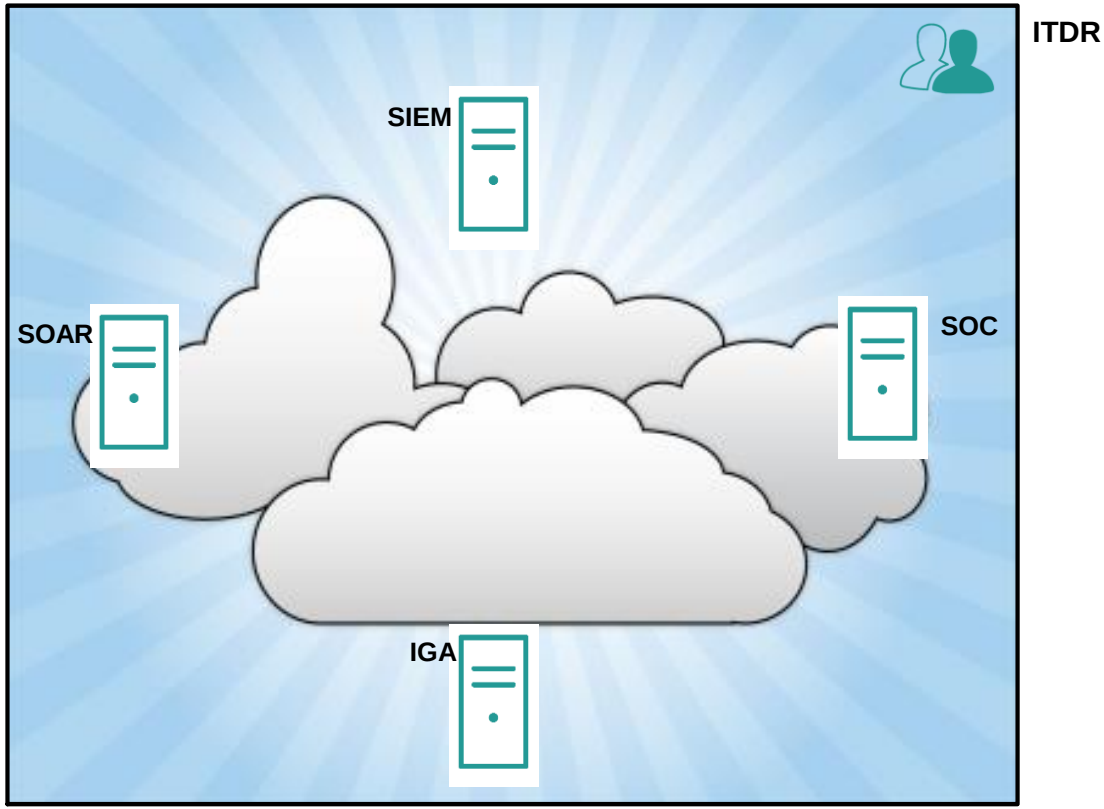
Identity Threat Detection and Response



Identity Threat Detection and Response



Identity Threat Detection and Response



Response

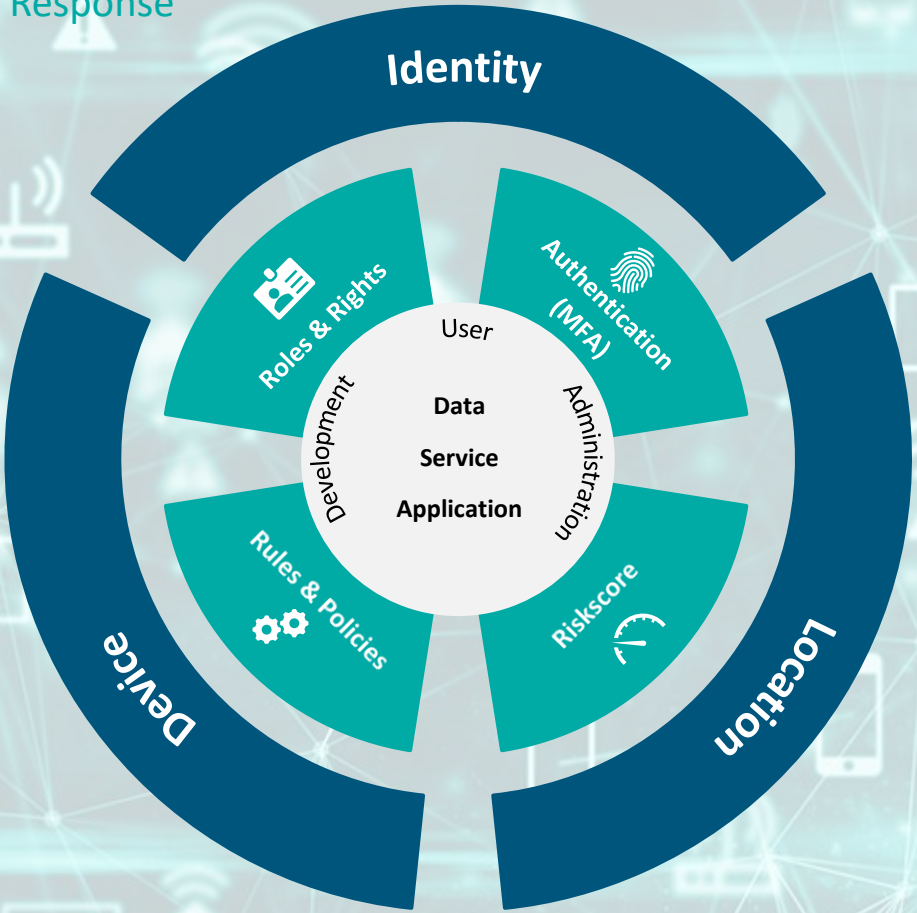
- Feedback / Verification
- Adaptive-Authentication
- Disable Account
- Session Blocking
- Single Sign off

Teil 3

Trends & Perspektiven

3

Zero Trust @ CONET



Shared Signals Framework (SSF)

Risk Incident Sharing and Coordination (RISC)

SETs

Continuous Access Evaluation Protocol (CAEP)

Shared Signals Working Group
OpenID Foundation

Transmitters/ Receivers API

Interoperability

SecEvents Subject Identifiers

Authentifizierung

- MFA als Teil von ITDR???
- Adaptive / Verhaltensbasierte Authentifizierung
- Kontinuierliche Authentifizierung
- z.B. Tastenanschläge, Mausbewegungen, Biometrie

Trends

- Bestehende xDR Systeme fokusieren zunehmend den Aspekt Identität
- Die Datenmenge zur Einschätzung von Bedrohungen steigt
- Kontinuierliche Riskobewertung / Scoring anstatt Eventmanagement
- Reaktionen werden zunehmend automatisiert

Fazit

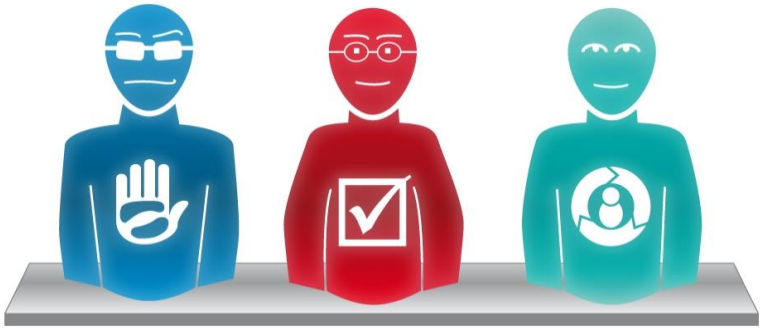
- ITDR ist ein neuer Ansatz Identitäten zu schützen
- Bestehende Lösungen können/müssen integriert werden
- Der Schutz von IAM-Systemen ist wichtiger als jemals zuvor
- ITDR ist ein weiterer Baustein der Cybersecurity


Noch Fragen?

Veranstaltungshinweis

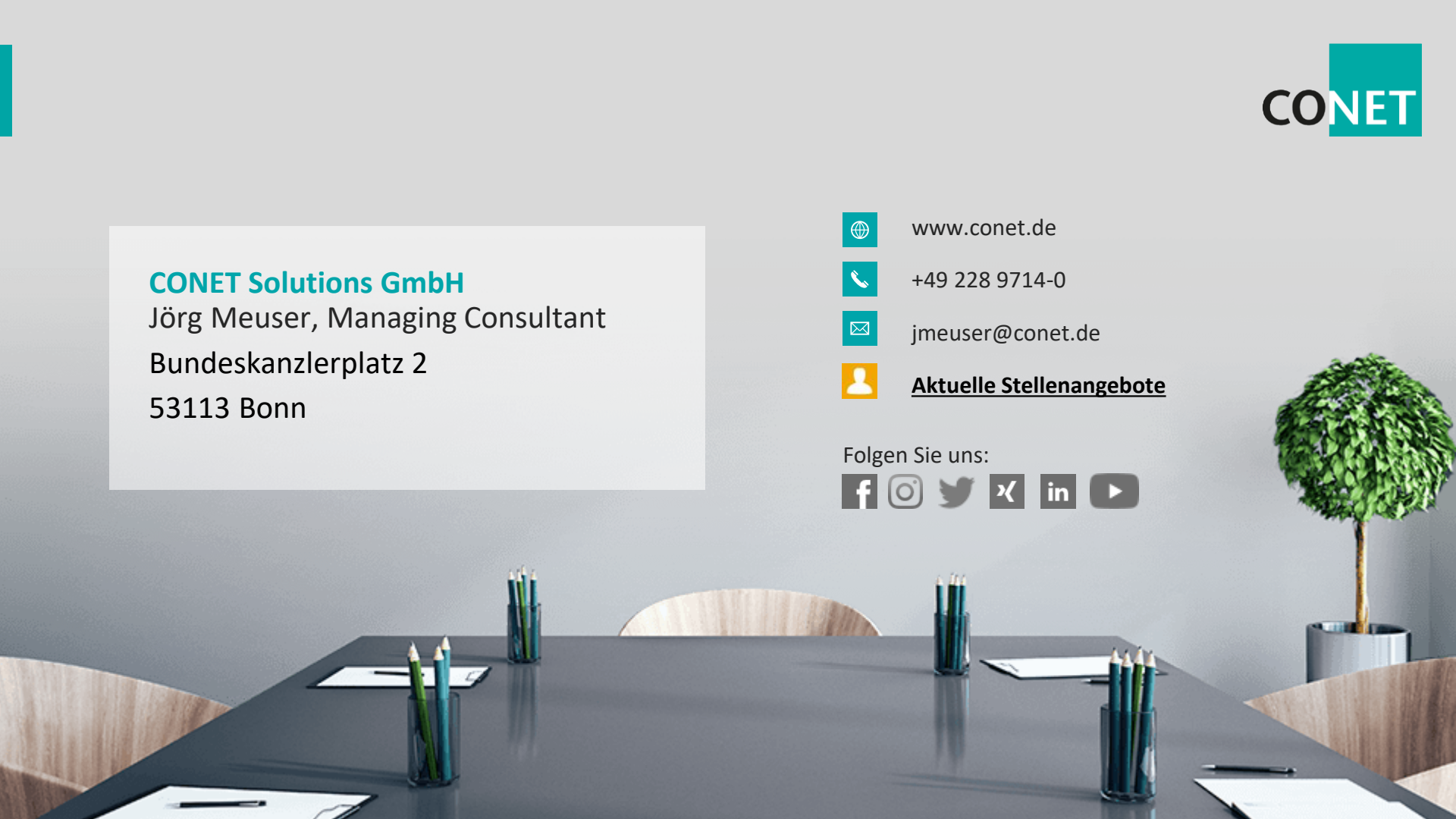
Dezentralisierte Identitäten

Einsatzmöglichkeiten für Unternehmen



Webinar, Donnerstag 29. August 2024, 11 bis 12 Uhr


CONET
Vielen Dank für Ihre Aufmerksamkeit!



CONET Solutions GmbH
Jörg Meuser, Managing Consultant
Bundeskanzlerplatz 2
53113 Bonn

www.conet.de
+49 228 9714-0
jmeuser@conet.de

Aktuelle Stellenangebote

Folgen Sie uns: