
OXFORD
COMPUTER GROUP
Hacker schlafen nie – wir auch nicht!
UNIVERSITÄT ZU LÜBECK
IDABUS®
TD SYNNEX

Song

Hacker schlafen nie – wir auch nicht!

Hacker schlafen nie – wir auch nicht

TD SYNNEX

SECUINFRA

OXFORD COMPUTER GROUP

Agenda

01 Vorstellung TD SYNNEX & SECUINFRA

02 Warum Security?

03 Demo SOC mit Integration IDABUS

TD SYNNEX | Microsoft Solutions Partner

Microsoft Solutions Partner
Frontier Distributor

Cloud-Geschäft mit dem weltweit größten Distributor? Darum mit TD SYNNEX.

Microsoft Frontier Distributor Designation – ein starkes Signal für Partner, die Cloud, Security & AI skalieren wollen.

1

Globale Stärke, lokale Nähe

Partner profitieren von weltweiter Skalierung und regionaler Betreuung.

2

Microsoft Cloud Expertise

Validierte Fähigkeiten rund um Cloud, AI, Security und CSP.

3

Schnelleres Wachstum für Partner

Enablement, Plattformen und Services helfen beim Ausbau des Cloud-Geschäfts.

4

Weniger Komplexität

Standardisierte Prozesse, Support-Modelle und digitale Plattformen reduzieren Reibung.

5

Mehr Vertrauen im Markt

Die Frontier Distributor Designation unterstreicht geprüfte Leistungsfähigkeit und Partner-Fokus.

TD SYNNEX

Taking Cyber-Security Personal

Sicherheit bei TD SYNNEX

TD SYNNEX

Organisatorische Maßnahmen

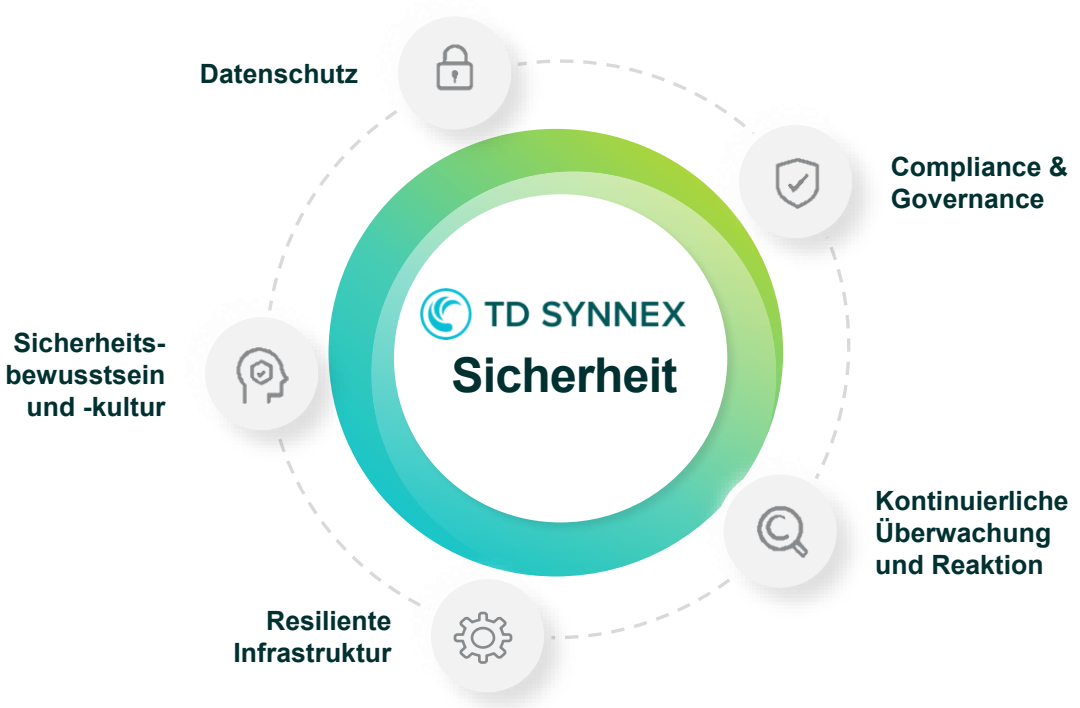
NIST-Rahmenwerk für Cybersicherheit

Information-Sharing und Analyse Centers (ISACs)

Regelmäßige Sicherheitsschulungen für Mitarbeiter

Incident-Response-Pläne und regelmäßige *Tabletop-Übungen.

Regelmäßige Penetrationstests und Sicherheitsaudits



Technische Maßnahmen

Ende-zu-Ende-Verschlüsselung

MFA-Durchsetzung

Zero-Trust-Zugriffskontrollen

Schwachstellen-Scanning und Patch-Management

Sicherer Softwareentwicklungslebens-zyklus (SSDLC)

*Tabletop-Übungen (auch Tabletop Exercises, kurz TTX) sind eine Form von Planspielen oder simulierten Krisenübungen, die typischerweise in einem Besprechungsraum (daher „Tabletop“) durchgeführt werden. Sie dienen dazu, Notfallpläne, Entscheidungsprozesse und die Zusammenarbeit zwischen verschiedenen Akteuren in einer simulierten Krisensituation zu testen und zu verbessern.

TD SYNNEX | Microsoft

Ihr Wechsel zu Microsoft Azure CSP - einfach, sicher, ohne Umstellungsaufwand

OCG
Oxford
Computer
Group

Heute

Sie zahlen Azure aktuell per Enterprise Agreement oder Kreditkarte (Pay-as-you-go)

Wir übernehmen die Umstellung für Sie

OCG - Oxford Computer Group - Ihr Ansprechpartner

Persönliche Betreuung, Beratung und Support aus einer Hand – Ihre Azure-Umgebung bleibt technisch unverändert, es gibt keinen Aufwand für Sie und keine Ausfallzeit

im Hintergrund abgesichert durch TD SYNNEX als Microsoft Distributor

Nur der Vertrag ändert sich

Morgen

Microsoft Azure CSP – günstiger, persönlich betreut, gleiche Leistung

Kein technischer Aufwand

Keine Ausfallzeit

Ihre Daten und Konfigurationen bleiben erhalten

Persönlicher Ansprechpartner bei OCG

in Partnerschaft mit TD SYNNEX

Noch On-Premises?
Auch dafür haben wir die passende Lösung

Der Weg in die Cloud – in Ihrem Tempo

Heute:
On-Premises

Eigene Server im eigenen Rechenzentrum

Public Cloud

Vollständiger Umzug nach Microsoft Azure – maximale Flexibilität, Skalierbarkeit und Innovationsgeschwindigkeit.

Hybrid Cloud mit Azure Local

Workloads bleiben lokal auf eigener Hardware – zentrale Verwaltung und Innovationen direkt aus der Azure Cloud über Azure Arc.

TD SYNNEX begleitet OCG & Sie – Beratung, Architektur, Migration, Betrieb und Support aus einer Hand.

- **Passende Strategie für Ihren Bedarf**
- **Datenhoheit und Sicherheit**
- **Nahtlose Integration in Azure**
- **Persönliche Beratung und Presales-Support**

Mehr als Microsoft:
Technologie aus einer Hand

Wir unterstützen Kunden über Cloud-Plattformen und Hardware-Hersteller hinweg.

Von der Cloud bis zum Endgerät: Wir verbinden Plattformen, Infrastruktur und Services zu einer passenden Kundenlösung.

TD SYNNEX

TECHCARE 24X7 MICROSOFT

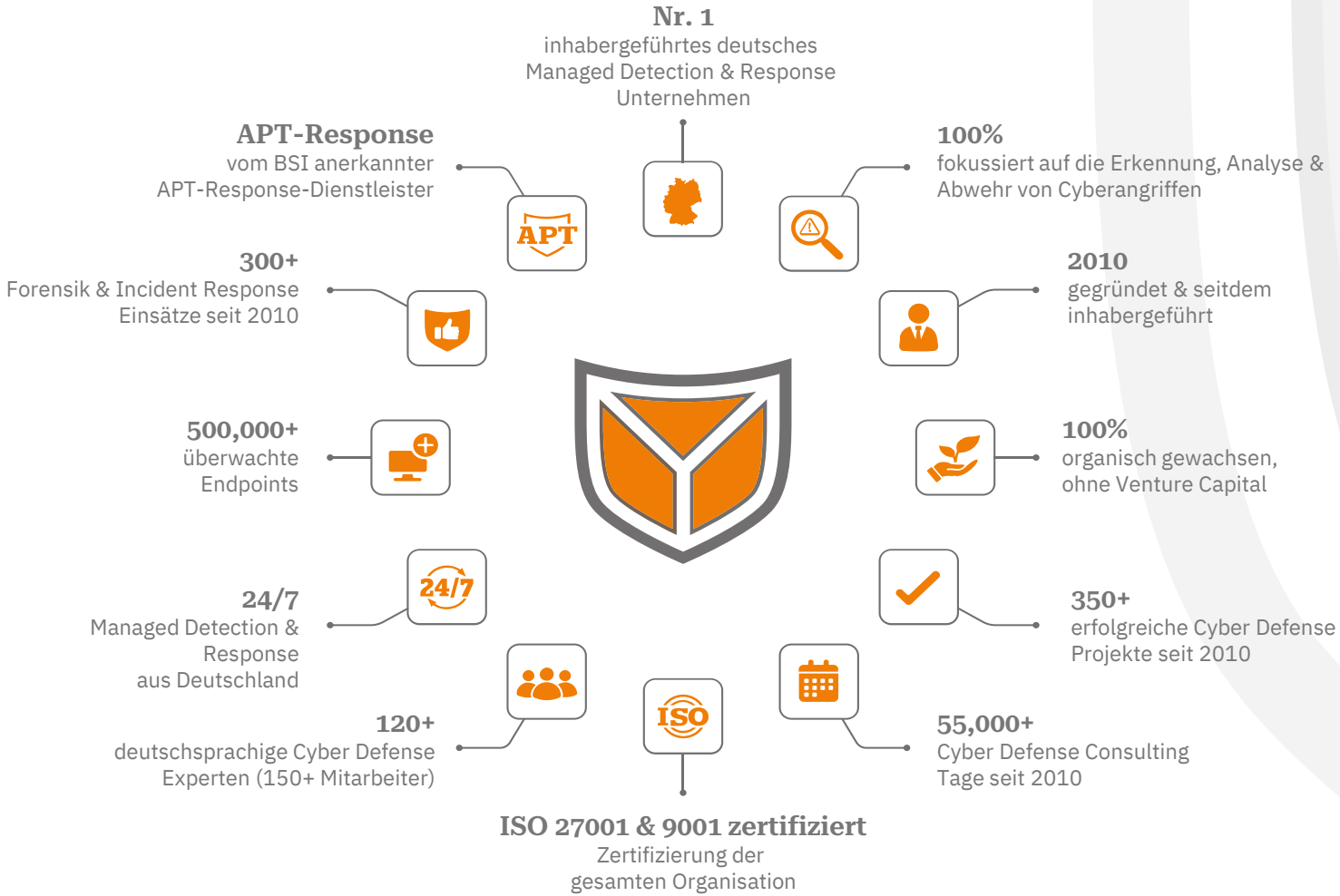
Microsoft-Support als Wachstumsmotor für Partner

Reaktiver technischer Support für Microsoft-Cloudtechnologien – mit 24x7-Verfügbarkeit in ELITE und Eskalationsweg zu Microsoft.

Ihr Support. Unsere Expertise. Ihr Wachstum.

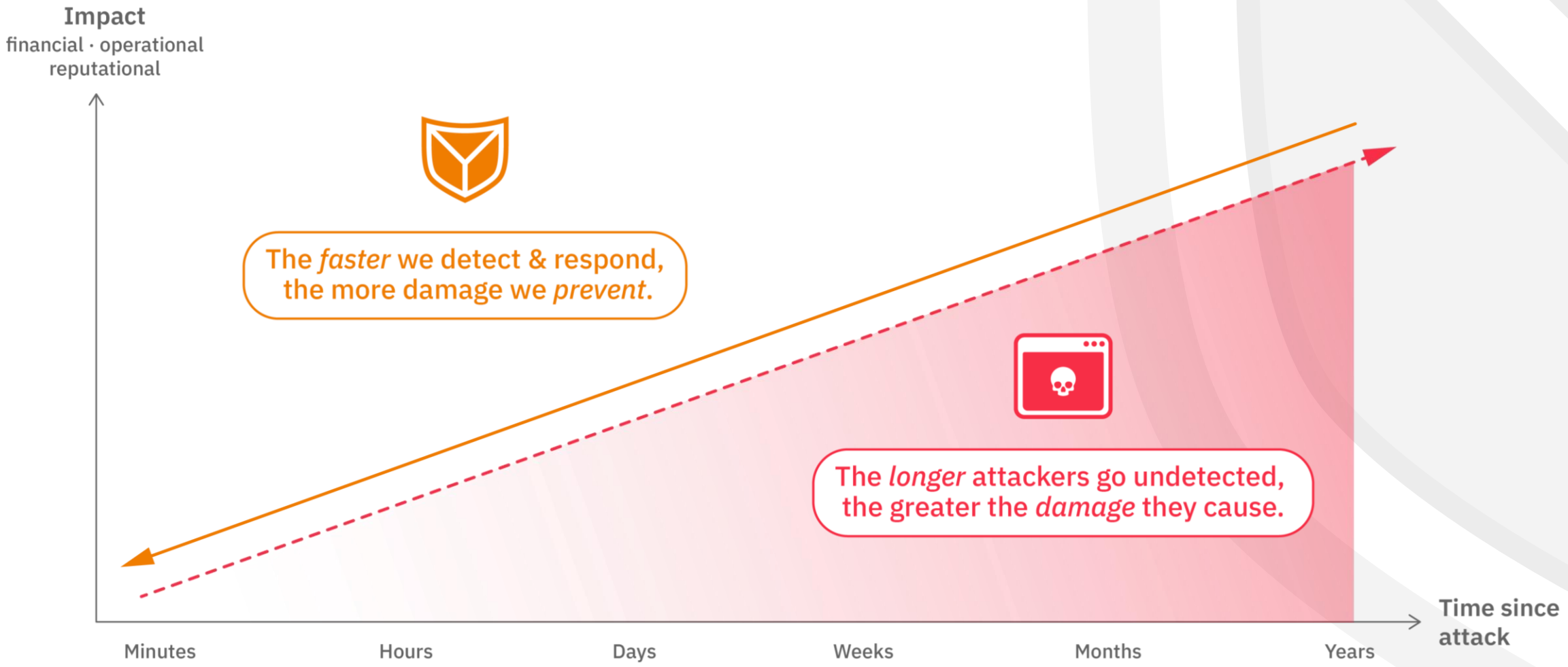
SECUINFRA auf einem Blick

Vertrauenswürdig. Spezialisiert. Unabhängig.



Detect. Respond. Defend.

Erkennungs- und Reaktionszeiten verkürzen, Schäden minimieren



AUSGANGSLAGE

Warum auch KMU heute moderne Security brauchen

Cyberangriffe treffen längst nicht mehr nur Konzerne.

Identitätsdiebstahl, Phishing-Kampagnen und Ransomware sind im KMU-Alltag angekommen – oft mit der gleichen Wucht wie im Enterprise.

Gleichzeitig fehlen vielen Unternehmen die Spezialisten, ein klassisches SOC und ein breit aufgestellter Security-Stack.

Die gute Nachricht: Microsoft 365 liefert heute bereits Security auf Enterprise-Niveau - modular, lizenzbasiert und für KMU passend gemacht.

Phishing

ist nach wie vor der häufigste Erstzugang – ein einziger Klick reicht.

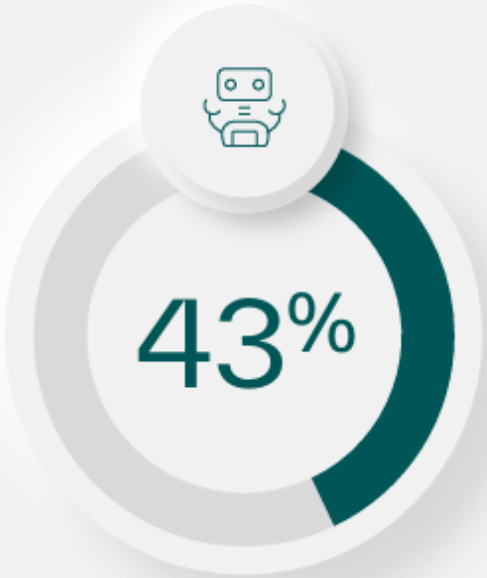
Identität

ist der neue Perimeter – kompromittierte Konten sind Hauptziel von Angreifern.

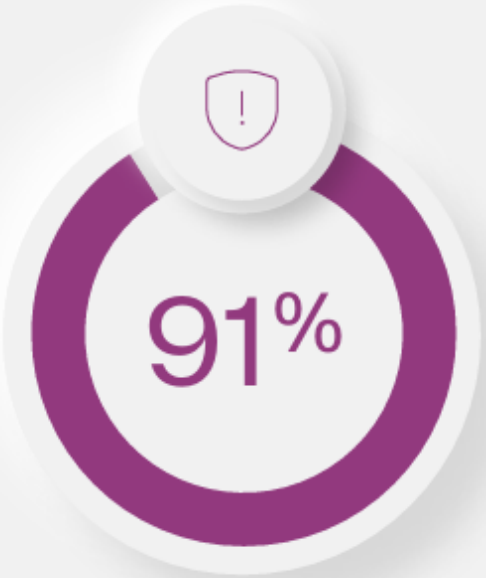
Geschwindigkeit

entscheidet – automatisierte Antwort schlägt manuelle Analyse.

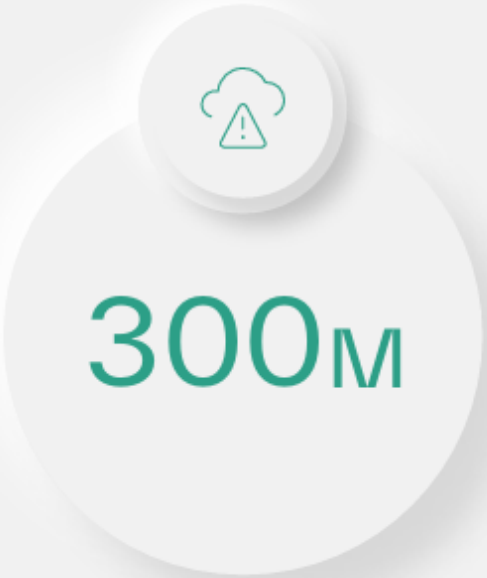
Kleine und mittelständische Unternehmen benötigen robuste Sicherheitslösungen, um Cyberbedrohungen zu minimieren und Betrug in der Cloud zu verhindern.



von allen Cyberangriffen richten sich gegen kleine und mittelständische Unternehmen



der Sicherheitsverletzungen entstehen häufig durch Phishing oder Spear-Phishing-Angriffe.

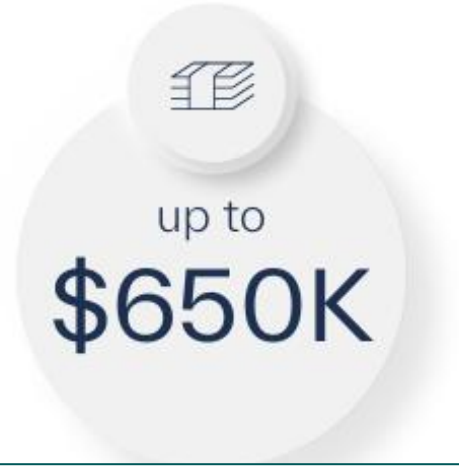


betrügerische Anmeldeversuche werden bei Microsoft-Cloud-Diensten täglich unternommen.

Sicherheitsbedenken für kleine und mittelständische Unternehmen (KMU)

Mit der zunehmenden medialen Aufmerksamkeit für Cyberangriffe wächst bei kleinen und mittelständischen Unternehmen das Bewusstsein für ihre Verwundbarkeit.

der kleinen Unternehmen halten ihre Cybersicherheitsstrategie für sehr effektiv



Im Durchschnitt geben kleine und mittelständische Unternehmen zwischen rund 770 € und 600.000 € für Cybersicherheitsvorfälle aus

Datum	€ Bußgeld	Empfänger	Land	Vergehen
03.06.2025	45.000.000 €	Vodafone	DE	Unzureichende Überprüfung und Überwachung von Unterauftragnehmern und Sicherheitsmängel im Onlineportal. »Details
01.10.2020	35.258.708 €	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	DE	Bespitzelung hunderter Mitarbeiter des Service Centers Nürnberg. »Details
03.03.2022	1.900.000 €	BREBAU GmbH	DE	Verarbeitung äußerst sensibler Daten von Mietinteressenten ohne Rechtsgrundlage. »Details
30.06.2020	1.240.000 €	AOK Baden-Württemberg	DE	Verwendung der Daten von 500 Gewinnspielteilnehmern für Werbezwecke. »Details
26.07.2022	1.100.000 €	Volkswagen	DE	Datenschutzverstöße beim Einsatz eines Dienstleisters zur Erprobung eines Fahrassistenzsystems. »Details
24.09.2021	901.389 €	Vattenfall Europe Sales GmbH	DE	Intransparente Datenabgleiche bei Vertragsanfragen für Neukunden-Sonderverträge in ca. 500 Tsd. Fällen. »Details
12.11.2024	900.000 €	Dienstleister	DE	Aufbewahrung personenbezogener Daten über Löschfristen hinaus. »Details
28.07.2022	900.000 €	Hannoversche Volksbank	DE	Auswertung von Kundendaten ohne Rechtsgrundlage. »Details
08.01.2021	900.000 €	notebooksbilliger.de AG	DE	Unrechtmäßige Videoüberwachung von Mitarbeitern und Kunden über einen Zeitraum von mindestens zwei Jahren. »Details

(*Summiert aus 27 Mio. + 15 Mio.)

https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

Microsoft

Bedrohungen sind real.
Wie Hochwasser am Fluss müssen wir sie erkennen, verstehen und beherrschen.

Security nicht dem Zufall überlassen:
Ganzheitliches Threat Modeling ist Pflicht

Security by Design beginnt mit einer Tatsache:
Bedrohungen bestehen – unabhängig von unserem Wunschdenken.

Baked-in Security über den gesamten Lebenszyklus

1. Verstehen
Bedrohungen identifizieren

2. Design
Mitigations in Architektur & Design integrieren

3. Umsetzen
Sicher entwickeln & sicher konfigurieren

4. Testen
Kontrollen validieren & Sicherheit verifizieren

5. Betreiben
Überwachen, Erkennen & Verbessern

6. Reagieren
Antworten, Eindämmen & Wiederherstellen

Ganzheitlicher Scope

- Assets
- Identitäten
- Datenflüsse
- Trust Boundaries
- Abhängigkeiten & Supply Chain
- Plattformen
- Betrieb & Monitoring
- Recovery & Resilienz
- KI-Systeme
- Modelle & Prompts
- Retrieval Content
- Agent Tools & Aktionen
- Berechtigungen & Identitäten (AI)

- Microsoft Azure
- Microsoft Entra
- Microsoft Defender for Cloud
- Microsoft Sentinel
- Microsoft Purview

Defense in Depth

- Sichere Identitäten & Zugriffskontrollen
- Netzwerk & Plattform Härtung
- Daten & Anwendungen schützen
- Erkennen & Überwachen (Detection)
- Eindämmen & Wiederherstellen (Response & Recovery)

Die bessere Frage ist nicht:
Haben wir ein Threat-Model-Dokument?

Die bessere Frage ist:
Sind die relevanten Bedrohungen verstanden, Mitigations umgesetzt, Kontrollen getestet und Response-Fähigkeiten im Betrieb belastbar?

Microsoft

Ein Kissen ist kein Airbag

VS.

Microsoft Defender

Credential Guard

Windows Hello

TPM

TPM 2.0

Windows 11

Microsoft 365

ZERO TRUST

Zero Trust

MODERNE SICHERHEITSARCHITEKTUR

✓ CRUMPLE ZONE
✓ ESP
✓ SENSOREN

Patch. **Upgrade.** **Redesign.** — Stay current, not just patched.

Microsoft Solutions Partner

Frontier Distributor

Windows Server 2025 Hotpatching mit Azure Arc

HOTPATCHING OHNE EXTRA-KOSTEN

Sicherheitsupdates im laufenden Betrieb. Weniger Downtime. Schnellere Absicherung.

HERAUSFORDERUNG
Regelmäßige Neustarts erzeugen Wartungsfenster und erhöhen bei Verzögerungen das Sicherheitsrisiko.

LÖSUNG
Azure Arc-fähiges Hotpatching installiert viele Sicherheitsupdates ohne Neustart direkt im laufenden Betrieb.

BUSINESS VALUE

Weniger Downtime	Deutlich weniger geplante Ausfallzeiten
Schneller geschützt	Kritische Sicherheitslücken früher schließen
Zentral gesteuert	Azure Update Manager als Kontrollpunkt
Integriert	Defender for Cloud, Monitor und Policy

ERGEBNIS

12 → 4
typische Neustarts pro Jahr

Monatliche Hotpatches ohne Reboot
Quartalsweise Baseline-Updates mit Neustart

EMPFEHLUNG

Einen Windows Server 2025 mit Azure Arc anbinden und Hotpatching pilotieren.

EXECUTIVE MESSAGE

Hotpatching reduziert Downtime, beschleunigt die Absicherung und verursacht keine zusätzlichen Hotpatching-Kosten.

AGENTIC AI IST BEREITS DA.
IST IHRE SECURITY BEREITS 360°?

TD SYNNEX
Powering Possible

Vom Cyber-Zoo zum digitalen Immunsystem.

REALER VORFALL:
KI HAT MALWARE AUF PYPI VERÖFFENTLICHT.
15 ECHTE SYSTEME INFIZIERT.
ZWEI UNTERNEHMEN HATTEN ES NICHT BEMERKT.

DIGITALES IMMUNSYSTEM
INTEGRIERT • PROAKTIV • RESILIENT

VOLLE SICHTBARKEIT
Über alle Identitäten, Geräte, Daten und Apps

INTELLIGENTE ERKENNUNG
KI-gestützte Detection und Bedrohungsanalyse

AUTOMATISIERTE REAKTION
Schnell. Konsistent. Effektiv.

24/7 ÜBERWACHT
Managed SOC – wir haben Ihre Umgebung im Blick

SICHERHEIT IST KEIN PRODUKT.
ES IST EINE ARCHITEKTUR.

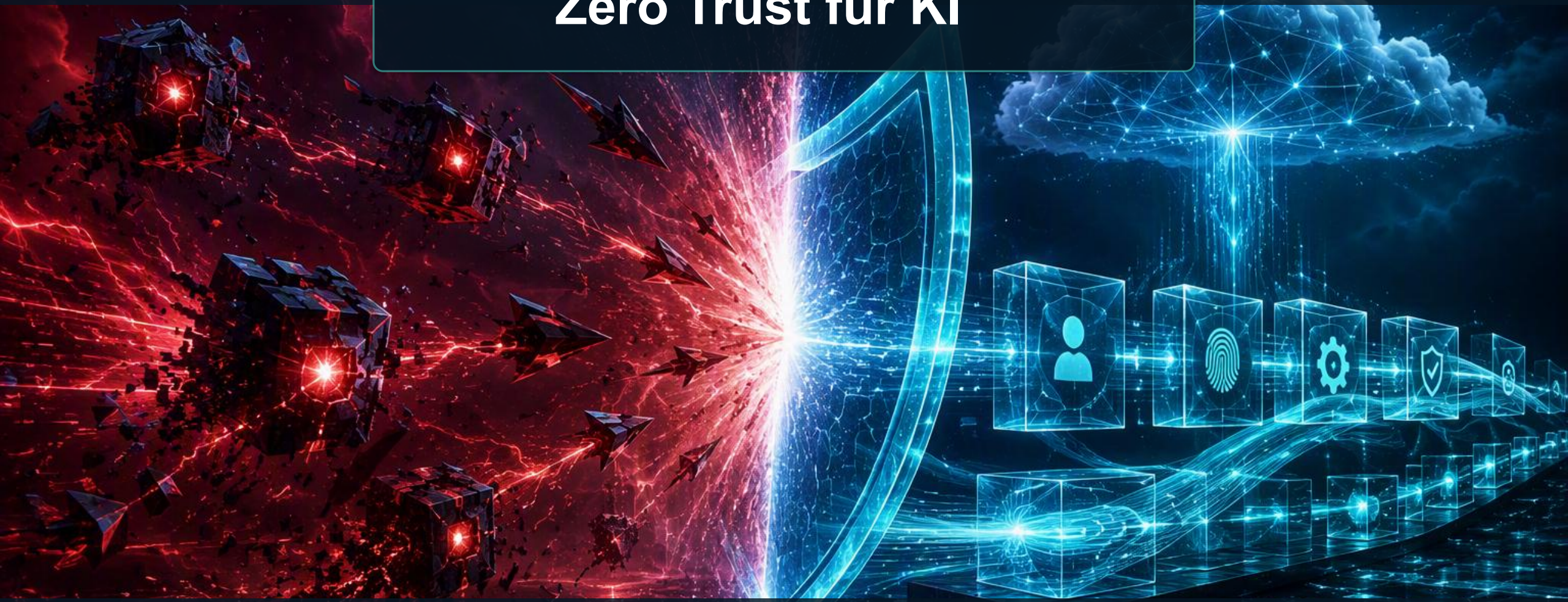
INTEGRIERT
Einheitliche Plattform statt Tool-Zoo

PROAKTIV
Bedrohungen erkennen, bevor sie Schaden anrichten

PARTNERSTARK
TD SYNNEX & Microsoft – gemeinsam für Ihren Erfolg

PRAKTISCH
Beratung, Assessments und Managed Services

Zero Trust für KI



KI-Sicherheit darf nicht als separates Spezialthema betrachtet werden. Sie muss in Identitätsmanagement, Datenschutz, Security Operations, Infrastruktur und insbesondere in den Softwareentwicklungsprozess integriert werden. KI beschleunigt Innovation und Entwicklung, erhöht aber gleichzeitig die Auswirkungen übermäßiger Berechtigungen, unsicherer Abhängigkeiten, mangelnder Governance und kompromittierter Software-Lieferketten.

Warum sollten Unternehmen ein SOC haben?

Früherkennung von Bedrohungen

Ein SOC überwacht kontinuierlich die IT-Infrastruktur auf Anzeichen von Cyberbedrohungen. Durch die Analyse von Netzwerkverkehr, Systemprotokollen und anderen Datenquellen können Angriffe frühzeitig erkannt werden, bevor sie großen Schaden anrichten können

Schnelle Reaktion und Abwehr

Ein SOC ermöglicht es einem Unternehmen, schnell auf Cyberangriffe zu reagieren. Durch eine gut koordinierte Reaktionsstrategie können Sicherheitsteams Angriffe isolieren, eindämmen und beseitigen, um den Schaden zu minimieren und die Ausfallzeiten zu reduzieren

Schutz sensibler Daten

Unternehmen verarbeiten und speichern sensible Kundendaten, Unternehmensgeheimnisse und andere vertrauliche Informationen. Ein SOC hilft, diese Daten vor Diebstahl, Leaks oder unbefugtem Zugriff zu schützen

Einhaltung von Vorschriften

Je nach Branche und Standort unterliegen Unternehmen verschiedenen gesetzlichen Vorschriften und Datenschutzbestimmungen. Ein SOC kann sicherstellen, dass die Sicherheitspraktiken des Unternehmens mit den Compliance-Anforderungen übereinstimmen und Audits erfolgreich bestanden werden

Risikomanagement und Business Continuity

Ein SOC trägt dazu bei, das Risiko für Cyberbedrohungen zu minimieren. Dies ist besonders wichtig, da erfolgreiche Angriffe nicht nur finanzielle Verluste verursachen, sondern auch den Ruf eines Unternehmens schädigen können. Durch die Reduzierung von Cyber-Risiken trägt ein SOC zur Aufrechterhaltung der Geschäftskontinuität bei

SECUINFRA

Cyber Defense. Made in Germany.

Demo: Bubble Balance Incident

Response in Idabus

OXFORD
COMPUTER GROUP

Bubble Balance

GmbH

Precision bubbles for perfectly level results

Monitoring

- SECUINFRA CDRC 24x7

Das Szenario

Die Beteiligten

cadmbeckert – IT-Administrator, Empfänger der Mail

rbernd (Rüdiger Bernd) – CEO, privilegierte Rollen, Critical Asset

Unbekannter Dritter – gibt sich als Bubble Balance HR aus

Das Setup

- HR-Impersonation-Mail an den Administrator
- Mehrere Alerts im XDR zur Identität rbernd
- Analyse und Response-Maßnahmen im IDABUS durch das SOC

Kein Exploit, keine Malware. Der Angriff läuft ausschließlich über legitime Identitätsfunktionen.

ID 247: Multi-stage incident involving Initial access & Persistence invo...

Manage incident | Tasks

High | Active | Unassigned | Unclassified | Last update time: 25 Aug 2026 09:20 | Critical asset

Attack story | Alerts (8) | Activities (14) | Assets (4) | Investigations (0) | Evidence and Response (4) | Summary

Filters: Severity: Any | Status: Any | Service sources: Any | Add filter

Detection & Categories

Active alerts
8/8

Categories
2

First activity
4 Aug 2026 13:00:00

Last activity
25 Aug 2026 09:10:32

Creation time
25 Aug 2026 08:47:38

Alerts

4 Aug 2026 13:00 • New
User Assigned to Privileged Role without MS-PIM
2 Users

25 Aug 2026 08:36 • New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...

25 Aug 2026 08:36 • New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...

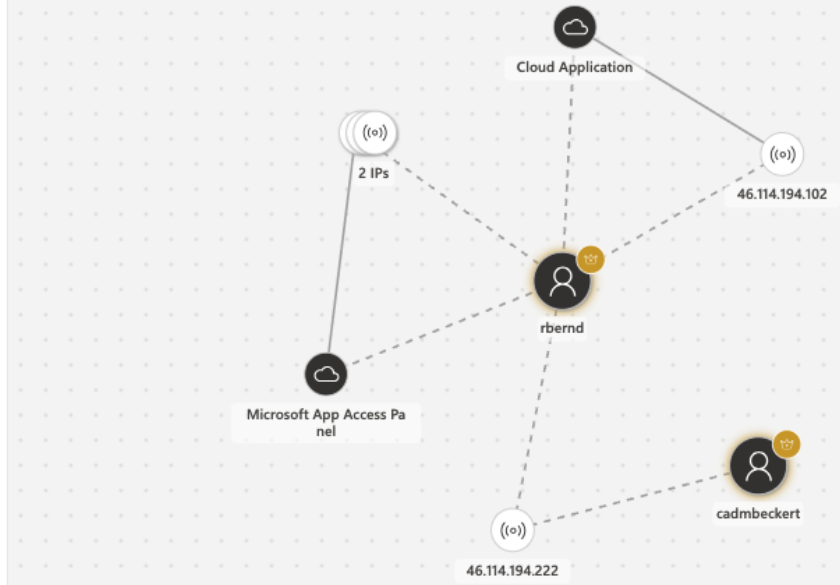
25 Aug 2026 08:36 • New
OCG_Authentication Method changed suspiciously
Rüdiger Bernd

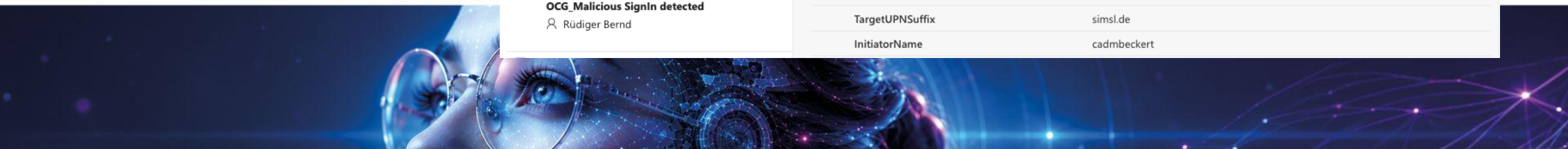
25 Aug 2026 08:41 • New
OCG_Malicious SignIn detected
Rüdiger Bernd

25 Aug 2026 08:41 • New
OCG_Malicious SignIn detected
Rüdiger Bernd

Incident graph

Layout | Group similar nodes | Entity types





Alerts

4 Aug 2026 13:00 New
User Assigned to Privileged Role without MS-PIM
2 Users

Category	Persistence
MITRE ATT&CK Techniques	T1078: Valid Accounts T1078.004: Cloud Accounts
Detection source	Scheduled detection
Service source	Microsoft Sentinel

25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...

25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...

25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger Bernd

25 Aug 2026 08:41 New
OCG_Malicious SignIn detected
Rüdiger Bernd

25 Aug 2026 08:41 New
OCG_Malicious SignIn detected
Rüdiger Bernd

25 Aug 2026 08:42 New
OCG_Malicious SignIn detected
Rüdiger Bernd

25 Aug 2026 09:10 New
OCG_Malicious SignIn detected
Rüdiger Bernd

Incident graph | Layout | Group similar nodes | Entity types

OCG_Authentication Method changed suspi... | User Assigned to Privileged Role without ...

Rule description

Identifies when a new eligible or active privileged role is assigned to a user. Does not alert on PIM activations. Any account eligible for a role is now being given privileged access. If the assignment is unexpected or into a role that isn't the responsibility of the account holder, investigate. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

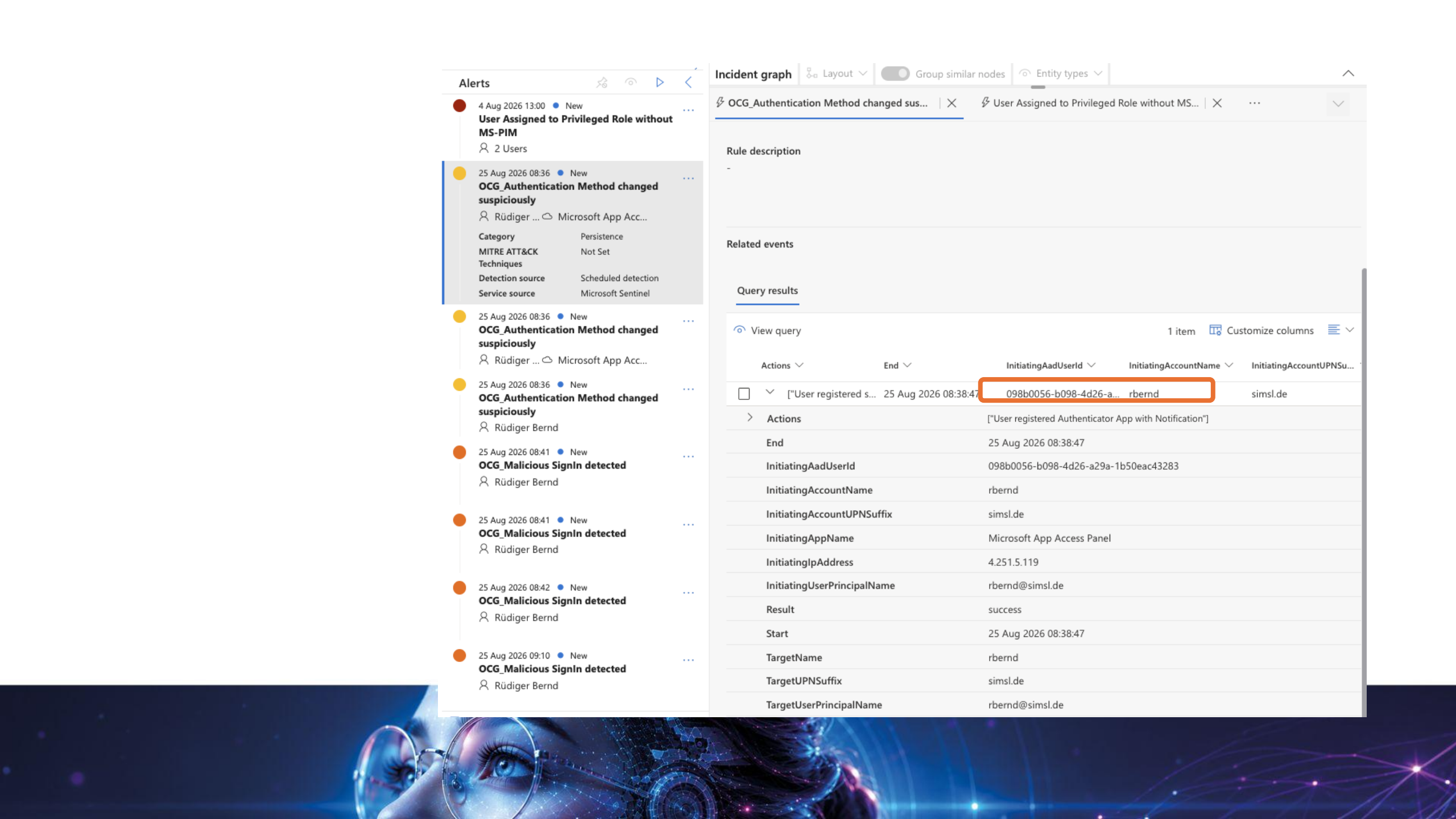
Related events

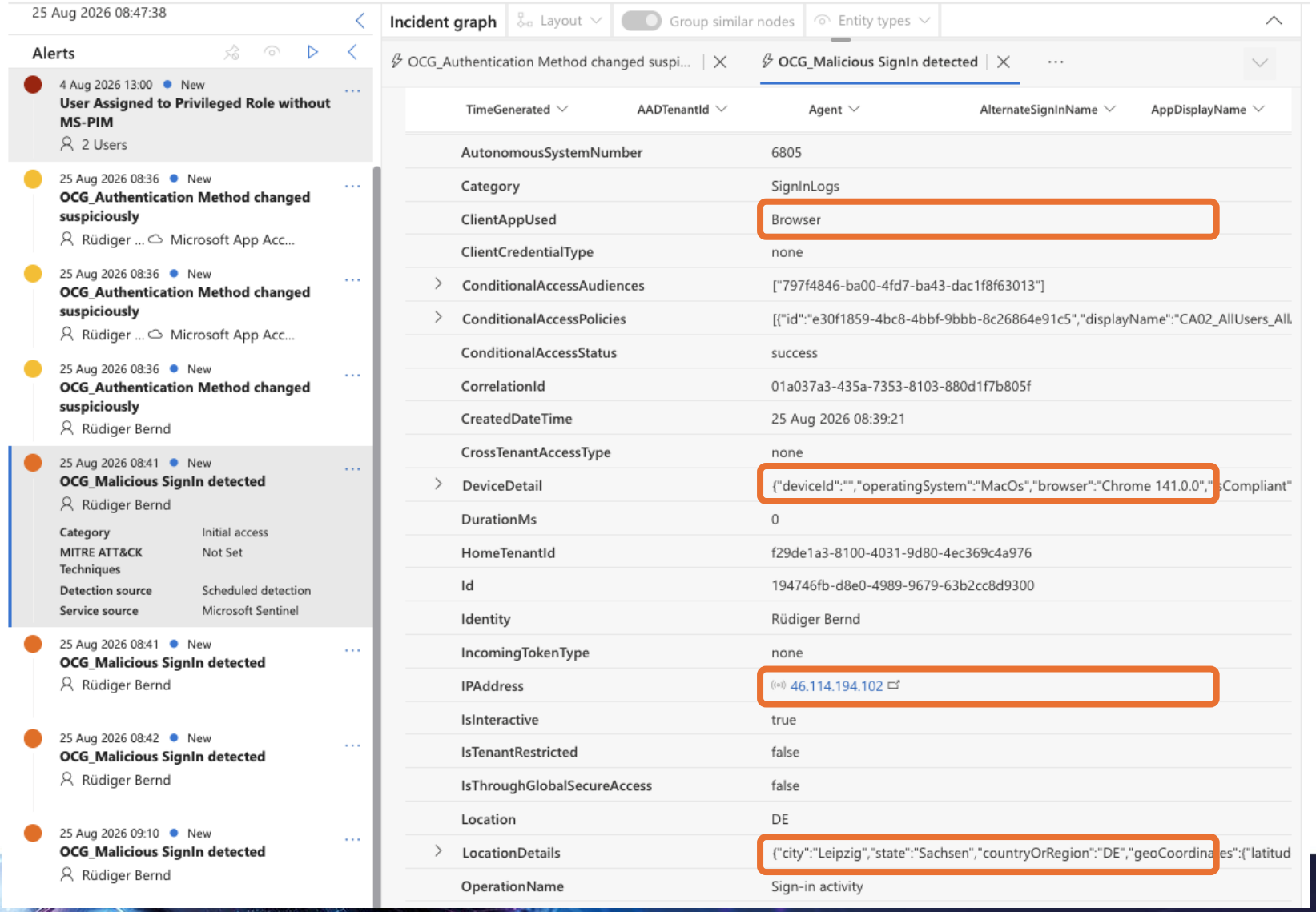
Query results

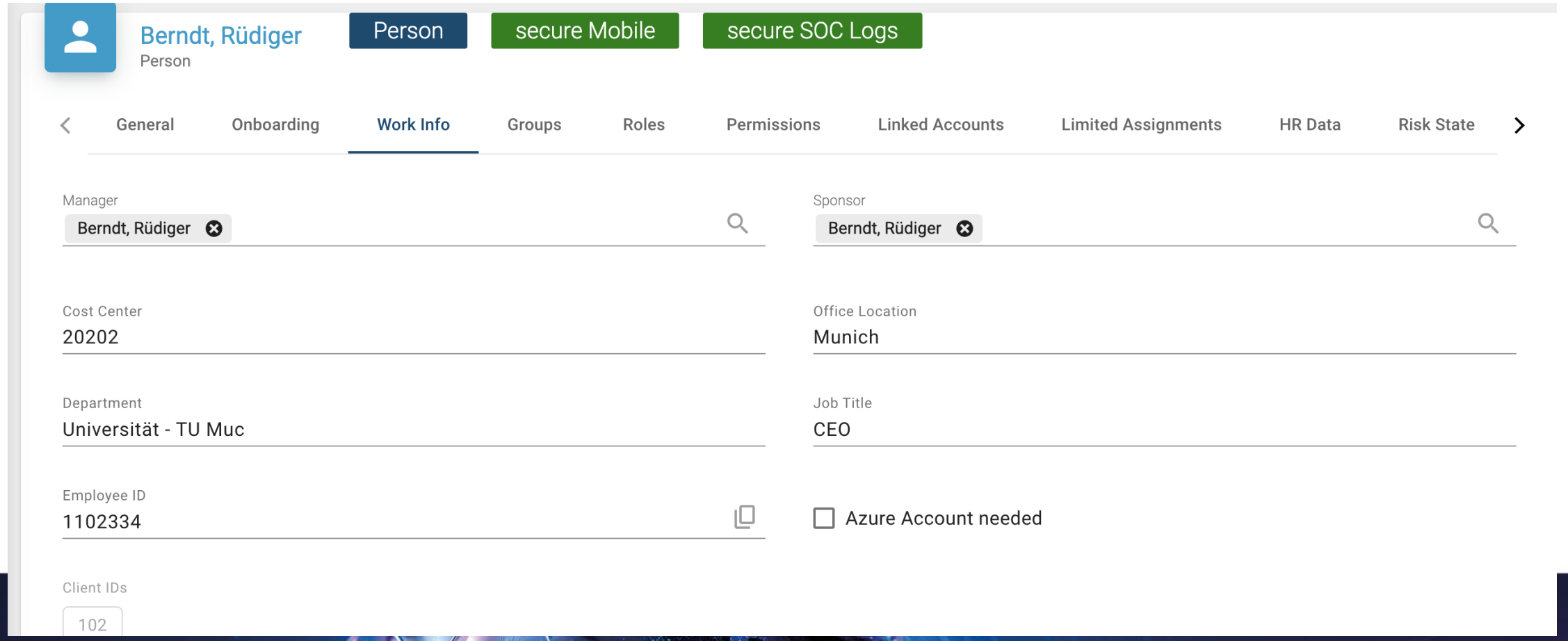
View query | 1 item | Customize columns

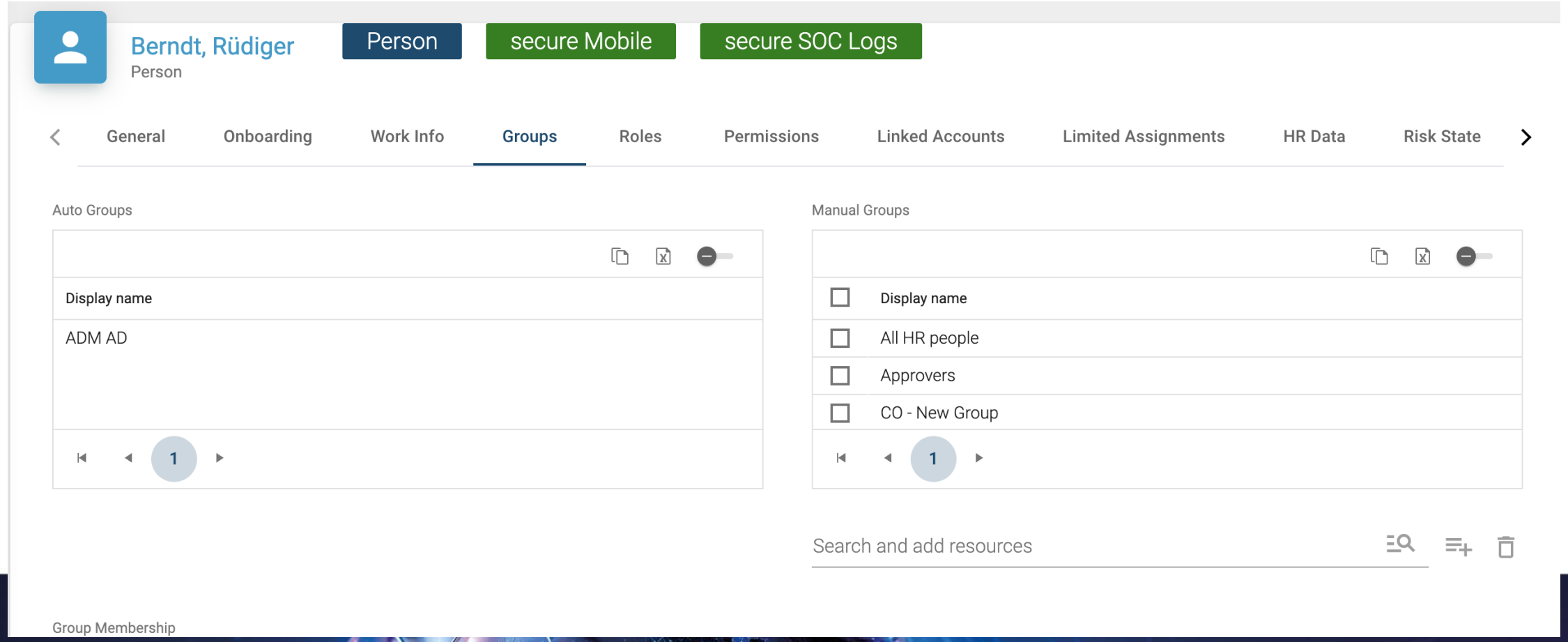
TimeGenerated	OperationName	RoleName	Target	Initiator
4 Aug 2026 13:00:00	Add member to role	Global Reader	rbernd@simsl.de	cadmbeckert@simsl.de

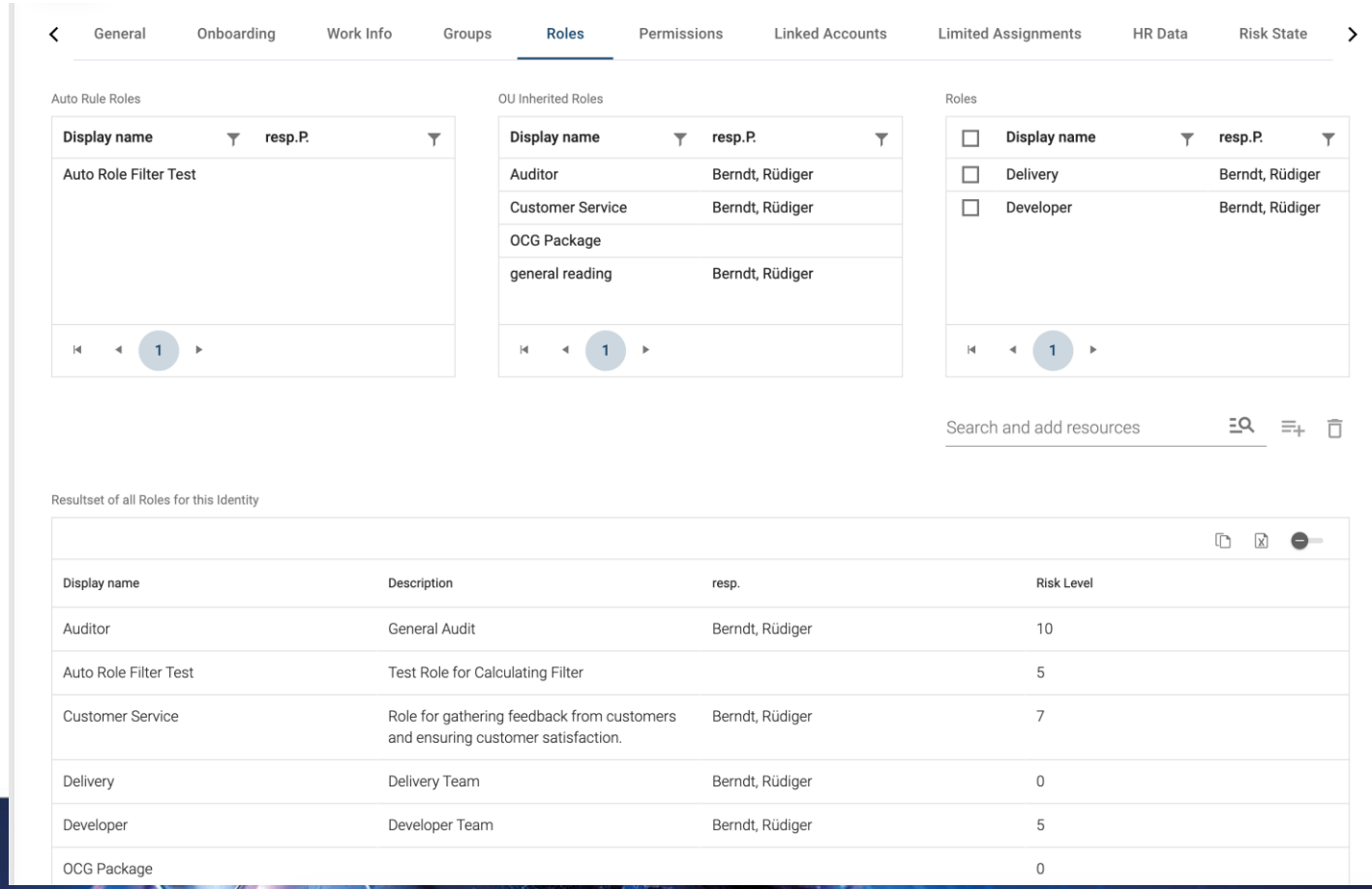
TimeGenerated	4 Aug 2026 13:00:00
OperationName	Add member to role
RoleName	Global Reader
Target	rbernd@simsl.de
Initiator	cadmbeckert@simsl.de
InitiatingUserPrincipalName	cadmbeckert@simsl.de
InitiatingAadUserId	37a47156-5922-4fa8-8d43-3376afe24a73
InitiatingIpAddress	46.114.194.222
Result	success
TargetName	rbernd
TargetUPNSuffix	simsl.de
InitiatorName	cadmbeckert

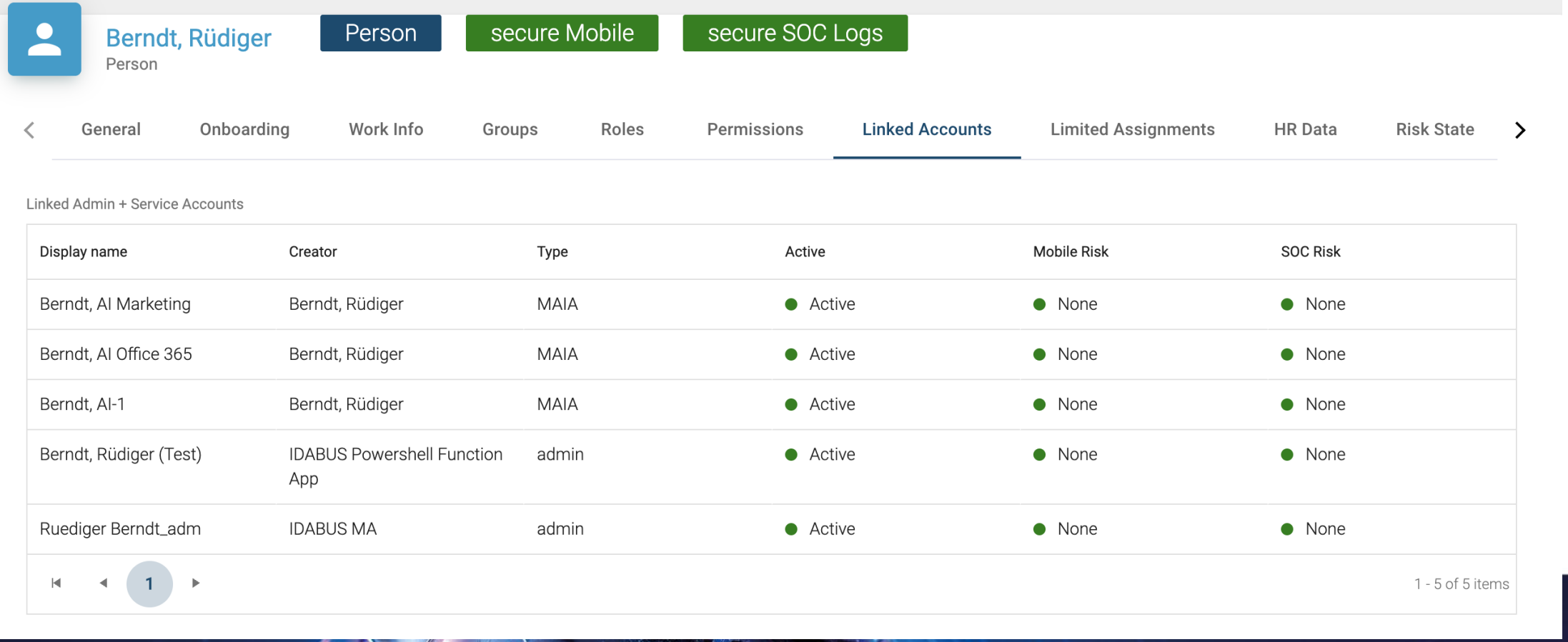

Alerts
4 Aug 2026 13:00 New
User Assigned to Privileged Role without MS-PIM
2 Users
25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...
Category Persistence
MITRE ATT&CK Techniques Not Set
Detection source Scheduled detection
Service source Microsoft Sentinel
25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...
25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger Bernd
25 Aug 2026 08:41 New
OCG_Malicious SignIn detected
Rüdiger Bernd
25 Aug 2026 08:41 New
OCG_Malicious SignIn detected
Rüdiger Bernd
25 Aug 2026 08:42 New
OCG_Malicious SignIn detected
Rüdiger Bernd
25 Aug 2026 09:10 New
OCG_Malicious SignIn detected
Rüdiger Bernd
Incident graph
Layout
Group similar nodes
Entity types
OCG_Authentication Method changed sus...
User Assigned to Privileged Role without MS...
Rule description
-
Related events
Query results
View query
1 item
Customize columns
Actions
End
InitiatingAadUserId
InitiatingAccountName
InitiatingAccountUPNSu...
["User registered s...
25 Aug 2026 08:38:47
098b0056-b098-4d26-a...
rbernd
simsl.de
Actions
["User registered Authenticator App with Notification"]
End
25 Aug 2026 08:38:47
InitiatingAadUserId
098b0056-b098-4d26-a29a-1b50eac43283
InitiatingAccountName
rbernd
InitiatingAccountUPNSuffix
simsl.de
InitiatingAppName
Microsoft App Access Panel
InitiatingIpAddress
4.251.5.119
InitiatingUserPrincipalName
rbernd@simsl.de
Result
success
Start
25 Aug 2026 08:38:47
TargetName
rbernd
TargetUPNSuffix
simsl.de
TargetUserPrincipalName
rbernd@simsl.de


25 Aug 2026 08:47:38
Alerts
4 Aug 2026 13:00 New
User Assigned to Privileged Role without MS-PIM
2 Users
25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...
25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger ... Microsoft App Acc...
25 Aug 2026 08:36 New
OCG_Authentication Method changed suspiciously
Rüdiger Bernd
25 Aug 2026 08:41 New
OCG_Malicious SignIn detected
Rüdiger Bernd
Category Initial access
MITRE ATT&CK Techniques Not Set
Detection source Scheduled detection
Service source Microsoft Sentinel
25 Aug 2026 08:41 New
OCG_Malicious SignIn detected
Rüdiger Bernd
25 Aug 2026 08:42 New
OCG_Malicious SignIn detected
Rüdiger Bernd
25 Aug 2026 09:10 New
OCG_Malicious SignIn detected
Rüdiger Bernd
Incident graph
Layout
Group similar nodes
Entity types
OCG_Authentication Method changed suspi...
OCG_Malicious SignIn detected
TimeGenerated
AADTenantId
Agent
AlternateSignInName
AppDisplayName
AutonomousSystemNumber 6805
Category SignInLogs
ClientAppUsed Browser
ClientCredentialType none
ConditionalAccessAudiences ["797f4846-ba00-4fd7-ba43-dac1f8f63013"]
ConditionalAccessPolicies [{"id":"e30f1859-4bc8-4bbf-9bbb-8c26864e91c5","displayName":"CA02_AllUsers_All
ConditionalAccessStatus success
CorrelationId 01a037a3-435a-7353-8103-880d1f7b805f
CreatedDateTime 25 Aug 2026 08:39:21
CrossTenantAccessType none
DeviceDetail {"deviceId":"","operatingSystem":"MacOs","browser":"Chrome 141.0.0","
Compliant"
DurationMs 0
HomeTenantId f29de1a3-8100-4031-9d80-4ec369c4a976
Id 194746fb-d8e0-4989-9679-63b2cc8d9300
Identity Rüdiger Bernd
IncomingTokenType none
IPAddress 46.114.194.102
IsInteractive true
IsTenantRestricted false
IsThroughGlobalSecureAccess false
Location DE
LocationDetails {"city":"Leipzig","state":"Sachsen","countryOrRegion":"DE","geoCoordinates":{"latitud
OperationName Sign-in activity









RB

Rüdiger Bernd

simsl.de | CEO | Enabled | OCG | Type: User | Criticality:

PRIVILEGED ENTRA PIM ROLES

Mark as compromised | Revoke session | ...

Overview | Incidents and alerts | Observed in organization | Risk score | **Timeline** | Identity Explorer | Security recommendations | Attack paths | Policies | Sentinel events

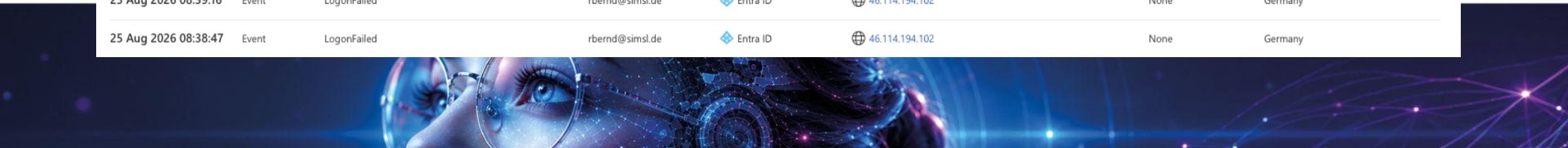
Export | Copy list link

30 items | Customize columns | 1 Week

Filter set: Filters: | Save

Type: Any | Title: Any | Source provider account ID: Any | Account display name: Any | Source provider: Entra ID, Microsoft Azure | IP address: Any | Add filter | Reset all | +4 more

Time	Type	Title	Account display name	Source provider	IP address	Device	Risk/Severity	Location	Tags
25 Aug 2026 08:39:23	Event	LogonSuccess	rbernd@simsl.de	Entra ID	46.114.194.102		None	Germany	
25 Aug 2026 08:39:22	Event	SSO Logon	Rüdiger Bernd	Microsoft Azure	46.114.194.102			Germany	
25 Aug 2026 08:39:22	Event	LogonSuccess	rbernd@simsl.de	Entra ID	46.114.194.102		None	Germany	
25 Aug 2026 08:39:21	Event	LogonFailed	rbernd@simsl.de	Entra ID	46.114.194.102		None	Germany	
25 Aug 2026 08:39:16	Event	LogonFailed	rbernd@simsl.de	Entra ID	46.114.194.102		None	Germany	
25 Aug 2026 08:38:47	Event	LogonFailed	rbernd@simsl.de	Entra ID	46.114.194.102		None	Germany	



Query Run query

```
1  EmailEvents
2  | where RecipientEmailAddress contains "beckert"
3  | where SenderFromAddress != @"mssecurity-noreply@microsoft.com"
4  | project SenderDisplayName, SenderFromAddress, coalesce(SenderIPv4, SenderIPv6), RecipientEmailAddress, Subject
```

Results | Query history | Getting started

Export | Show empty columns | 3 it

Filters: Add filter

SenderDisplayName	SenderFromAddress	Column1	RecipientEmailAdd...	Subject
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Bubble HR	felix.gutjahr@secuinfra.com	2a01:111:f403:c202::7	cadmbeckert@simsl.de	WICHTIG | Anlage Benutzer ...
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

2a01:111:f403:c202::7 (2a01:111:8000::/33)

AS 8075 (Microsoft Corporation)

SE

Last Analysis Date

7 days ago

WICHTIG | Anlage Benutzer Rüdiger Ber...

Open email entity | View header | Take action | ...

Email details

Sender display name
Bubble HR

Sender address
felix.gutjahr@secuinfra.com

Sender mail from address
felix.gutjahr@secuinfra.com

Sent on behalf of
-

Return path

Sender IP
2a01:111:f403:c202::7

Location
-

Recipient(s)
cadmbeckert@simsl.de

Time received (UTC +02:00)
26 Aug 2026 14:52

Directionality
Inbound

Network message ID
b2f78c22-6297-4963-6819-08df0370e8ac

Internet message ID
<AM9PR01MB7218369C60C6420143BE5DFFE0AE2@AM9PR01MB7218.eurprd01.prod.exchangelabs.com>

WICHTIG | Anlage Benutzer Rüdiger Berndt

Take action | Copilot | Download email | ...

Tags

Recipient tags

MikeOnly | SI remediation

Sender tags

Timeline | Analysis | Attachments | URL | Similar emails | **Email preview**

WICHTIG | Anlage Benutzer Rüdiger Berndt

Bubble HR <felix.gutjahr@secuinfra.com>
Wednesday 26 August 2026 at 14:52
To:<cadmbeckert@simsl.de>

smime.p7s
11.40 KB

Hallo Herr Beckert,

Bernd Rüdiger beginnt demnächst als neuer CEO in unserem Unternehmen.

Bitte entsprechend dem neuen CEO einen Account anlegen und das Initial Passwort zurück an mich senden - ich übergebe es dann.

Danke,

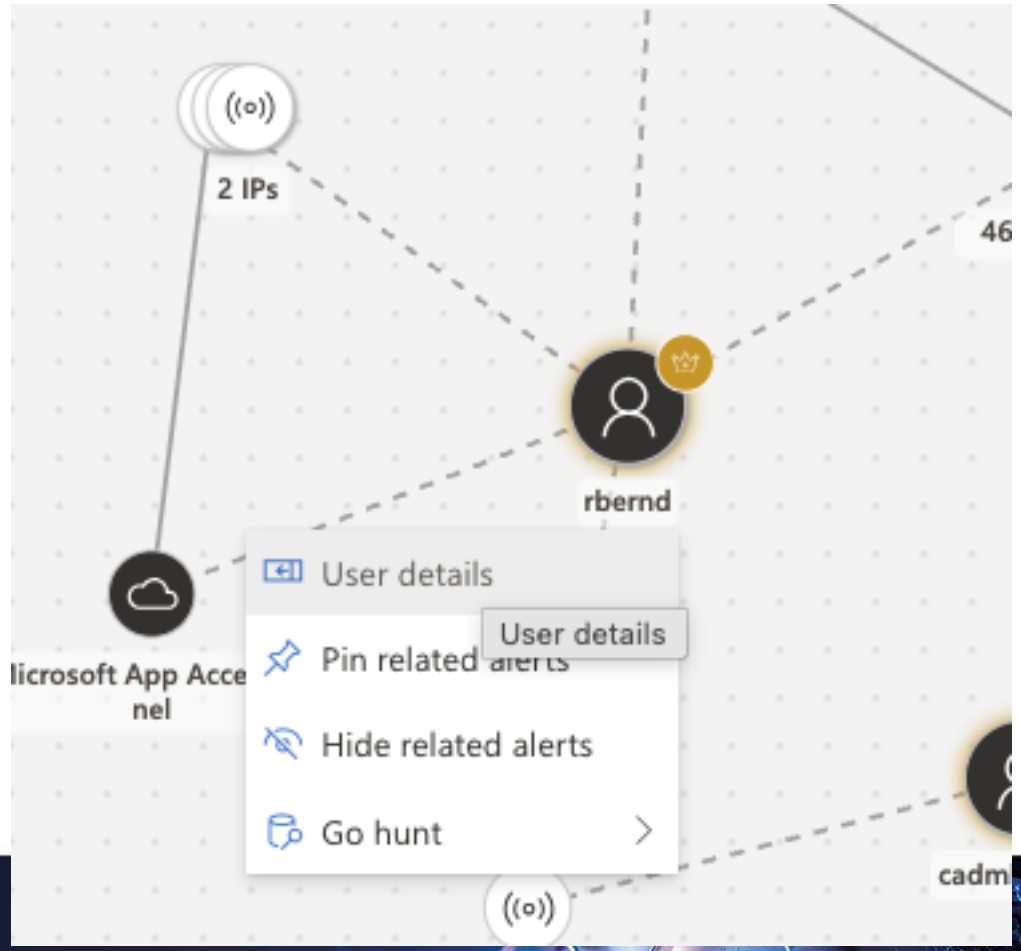
Bubble Balance GmbH

Bewertung

Warum wir das Konto als kompromittiert einstufen

1. **Phishing** – Admin fällt auf die Mail herein, Initialpasswort geht an den Angreifer, IAM-Prozesse werden nicht eingehalten
2. **Persistenz** – Anmeldung mit dem Initialpasswort und Registrierung einer eigenen MFA-Methode
3. **Zugriff** – Erfolgreiche Anmeldung von einer anderen IP, die nicht zu den Informationen aus IDABUS passt
4. **Auffällige Aktivität** – Unmittelbar danach Anmeldung in Microsoft Azure, untypisch für den CEO

Bewertung: Konto kompromittiert. Ein Passwort-Reset genügt nicht, die Reaktion muss die Identität selbst treffen.



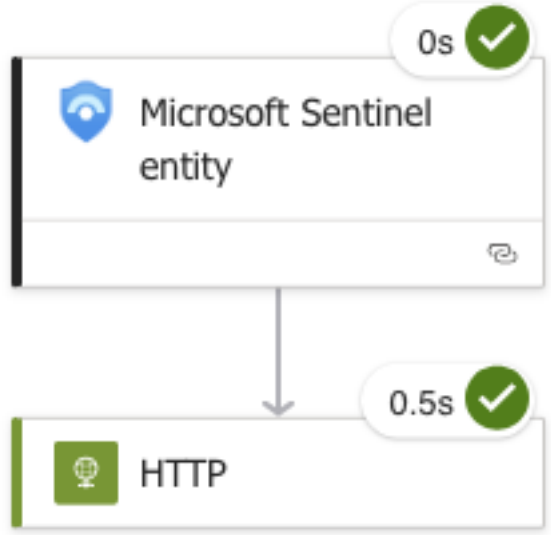
RB

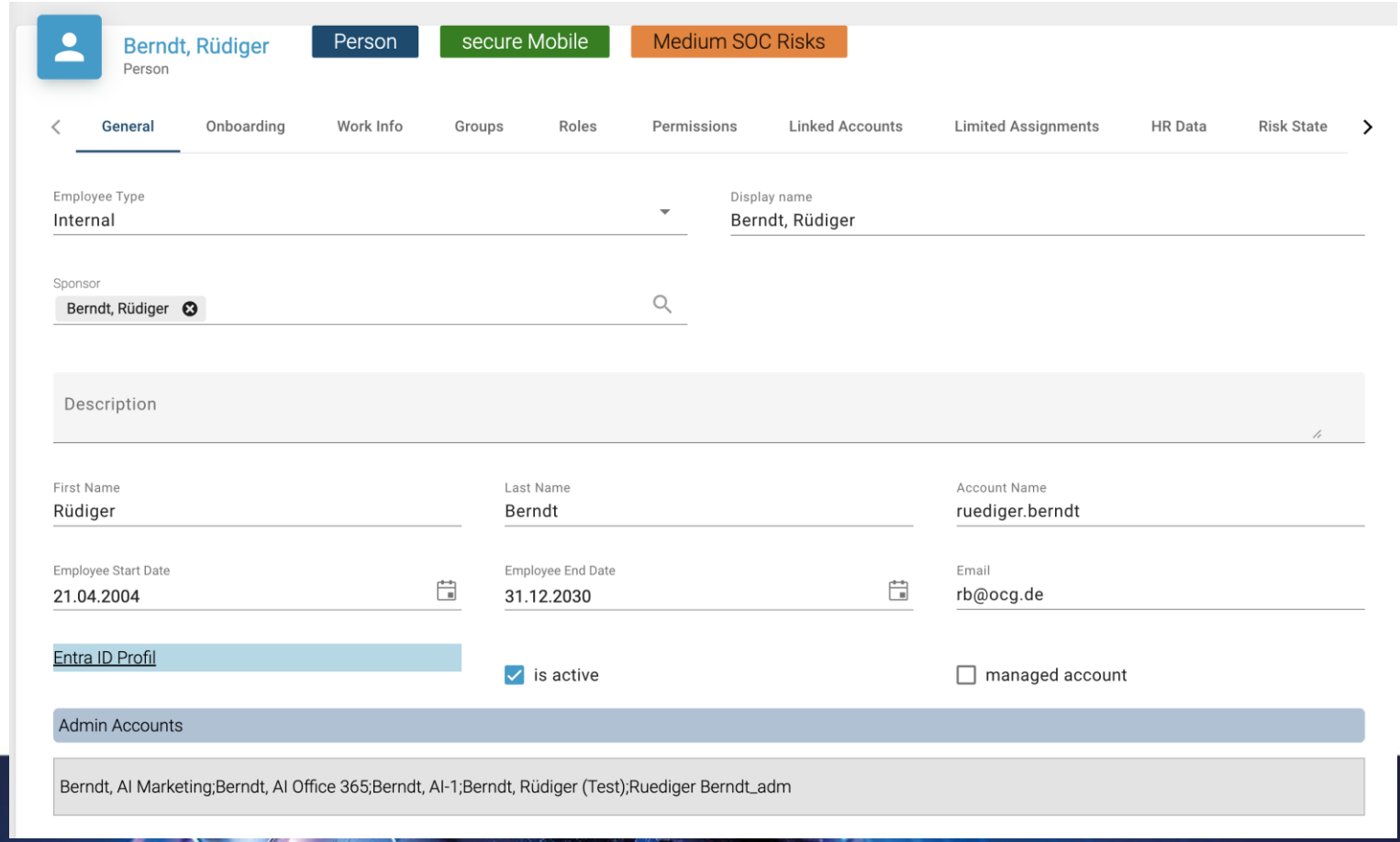
Rüdiger Bernd

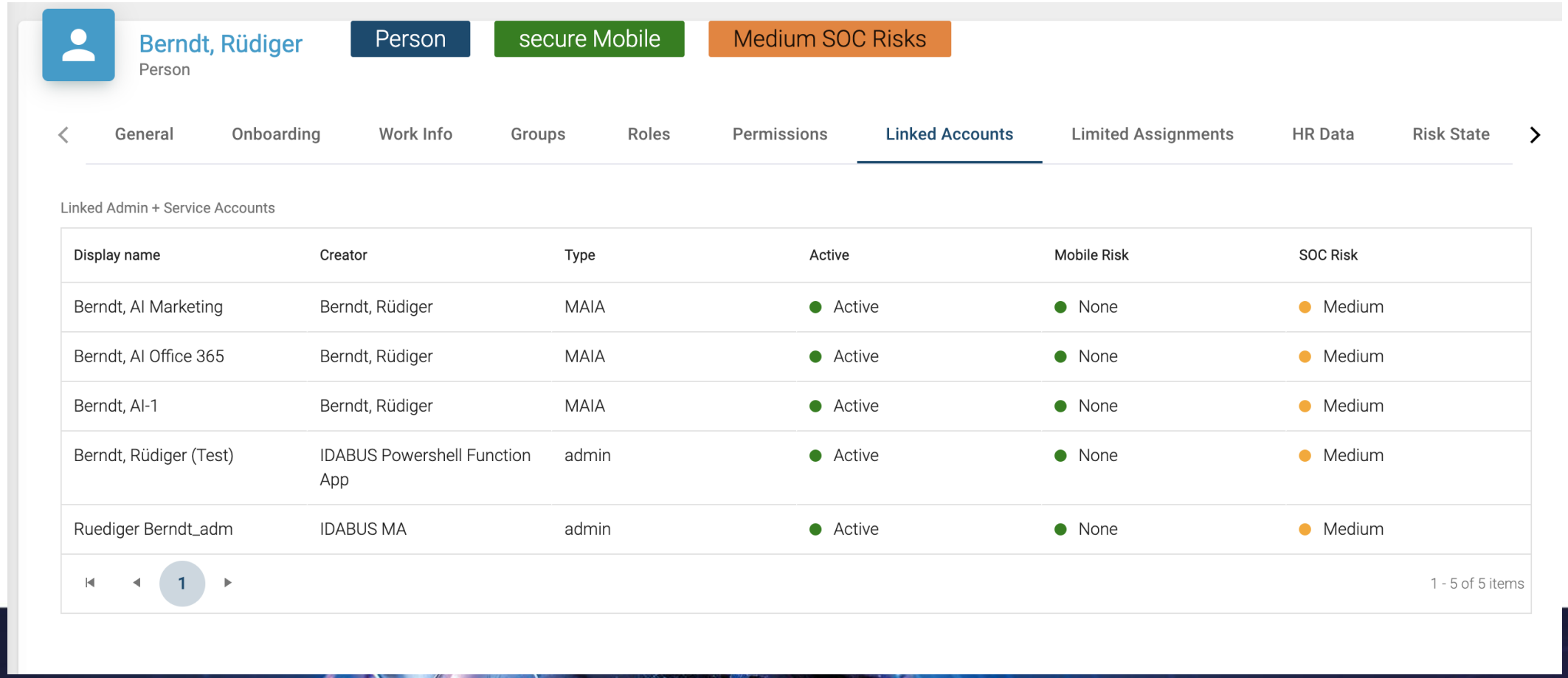
simsl.de | CEO | Enabled | +3

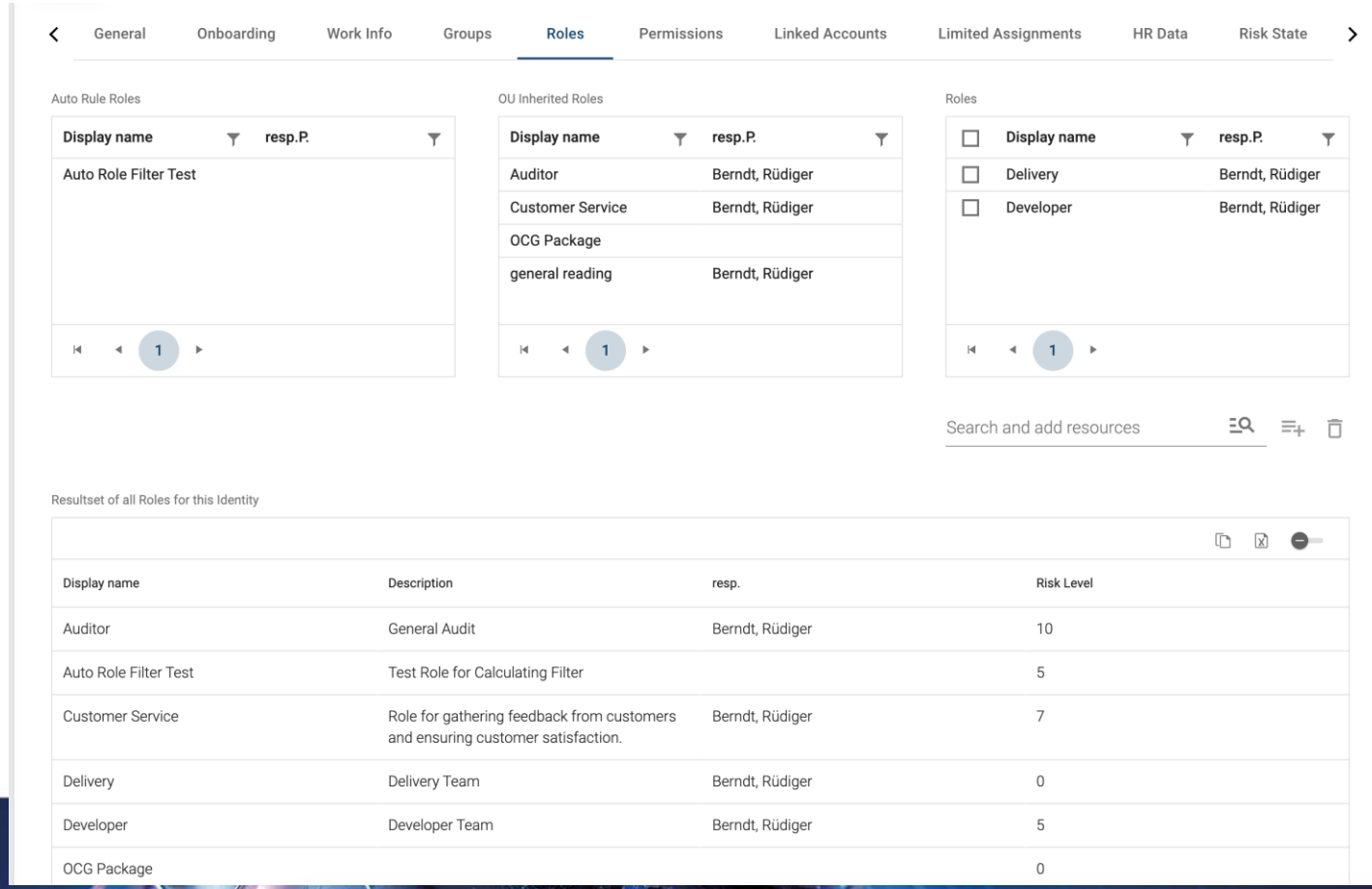
PRIVILEGED ENTRA PIM ROLES

Mark as compromised ...


0s
Microsoft Sentinel entity
0.5s
HTTP







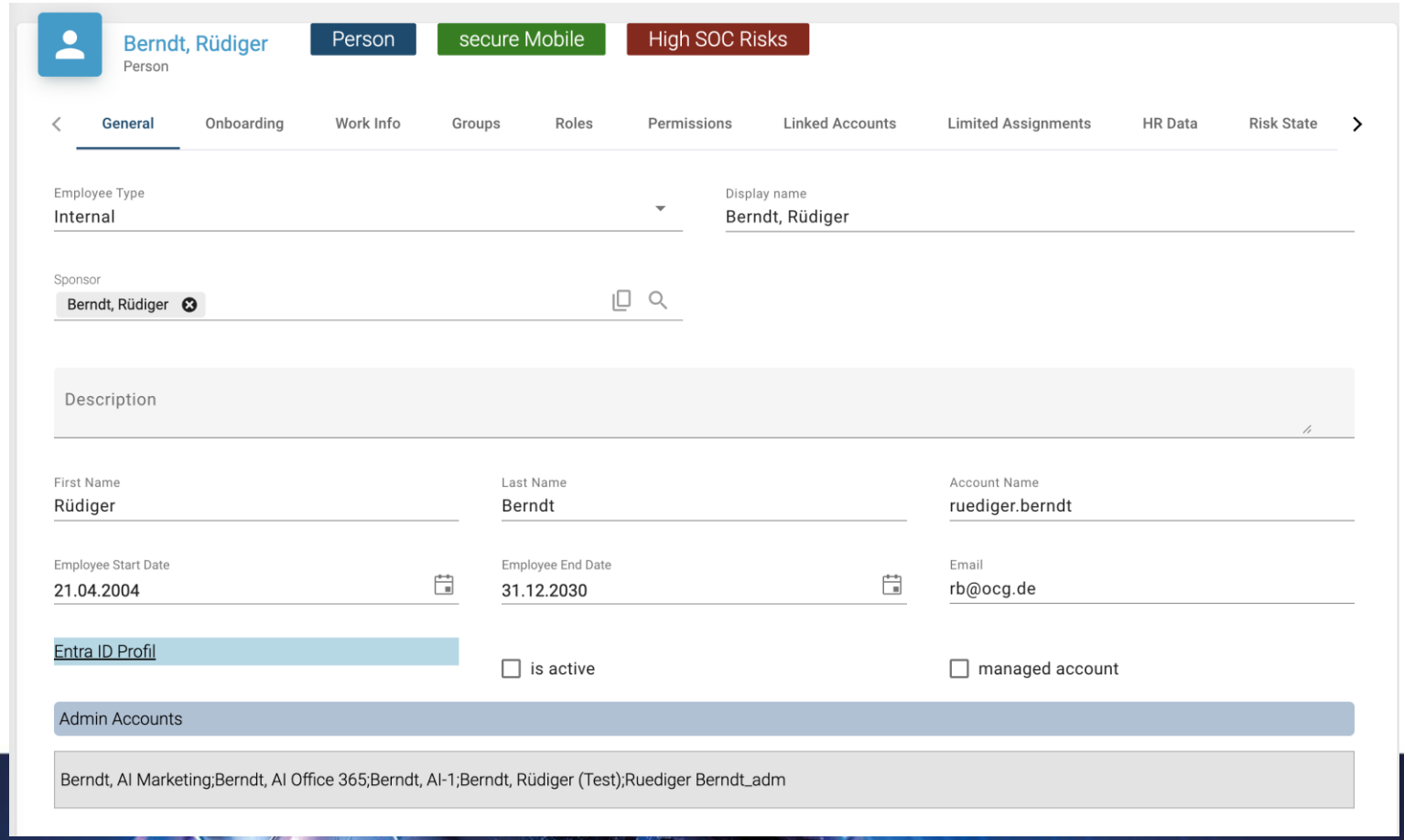
This User is in risk - some roles are removed from this user

Resultset of all Roles for this Identity

Display name	Description	resp.	Risk Level
Delivery	Delivery Team	Berndt, Rüdiger	0
OCG Package			0
general reading		Berndt, Rüdiger	1

1

1 - 3 of 3 items



Berndt, Rüdiger

Person

Person | secure Mobile | High SOC Risks

General | Onboarding | Work Info | Groups | Roles | Permissions | **Linked Accounts** | Limited Assignments | HR Data | Risk State

Linked Admin + Service Accounts

Display name	Creator	Type	Active	Mobile Risk	SOC Risk
Berndt, AI Marketing	Berndt, Rüdiger	MAIA	Inactive	None	High
Berndt, AI Office 365	Berndt, Rüdiger	MAIA	Inactive	None	High
Berndt, AI-1	Berndt, Rüdiger	MAIA	Inactive	None	High
Berndt, Rüdiger (Test)	IDABUS Powershell Function App	admin	Inactive	None	High
Ruediger Berndt_adm	IDABUS MA	admin	Inactive	None	High

1

1 - 5 of 5 items

Key Takeaways

Was wir aus dem Fall mitnehmen

1 Identität ist der Angriffsvektor

Kein Exploit, keine Malware. Der Angriff lief über legitime Funktionen: Rollenzuweisung, Passwortweitergabe, MFA-Registrierung.

2 Zeit entscheidet über den Schaden

Erkennung und Reaktion erfolgten unmittelbar nach der MFA-Registrierung, vor Datenzugriff und weiterer Ausbreitung.

3 Der Risk Score macht die Reaktion abgestuft

Medium provisioniert Rollen zurück, High sperrt Konto und verknüpfte Accounts. Nicht jeder Verdacht führt zur Vollsperrung.

4 Verknüpfte Konten sind der Hebel

Eine Sperrung nur in Entra lässt die Identität in allen anderen Systemen unangetastet.

Der Angriff wurde gestoppt, bevor Schaden entstanden ist. Genau dafür braucht es Erkennung und Reaktion rund um die Uhr.

17. SECURITY & EFFICIENCY SUMMIT 2026

3. – 4. SEPTEMBER 2026 ERDING

DANKE FÜR IHRE TEILNAHME!

Praxis. Partnerschaft.
Sicherheit rund um die Uhr.

- MODERNE SECURITY
- EXPERTEN AUSTAUSCH
- PRAXISNAHE LÖSUNGEN
- IDENTITY & ACCESS SECURITY

24/7

VERNETZEN.
AUSTAUSCHEN.
VORANKOMMEN.

ANDREAS WOLFFS
TD SYNNEX

FELIX GUTJAHR
SECUINFRA

ERDINGER WEISSBRÄU
ERDINGER Weißbräu HERBSTFEST

GEMEINSAMER BESUCH DES ERDINGER HERBSTFESTS IM WEISSBRÄU-ZELT

Netzwerken. Austausch. Genießen.