tenable

Cyber Exposure im OT-Umfeld:

Wie Tenable verwundbare Systeme und ausnutzbare Schwachstellen identifiziert

Mehr als Schwachsellen: Exposure

Exposure ist ein vermeidbares Cyber-Betriebsrisiko, das mit einer hohen Wahrscheinlichkeit von Angreifern ausgenutzt wird UND das Potential hat, wesentlichen Einfluss auf den Betriebserfolg zu nehmen

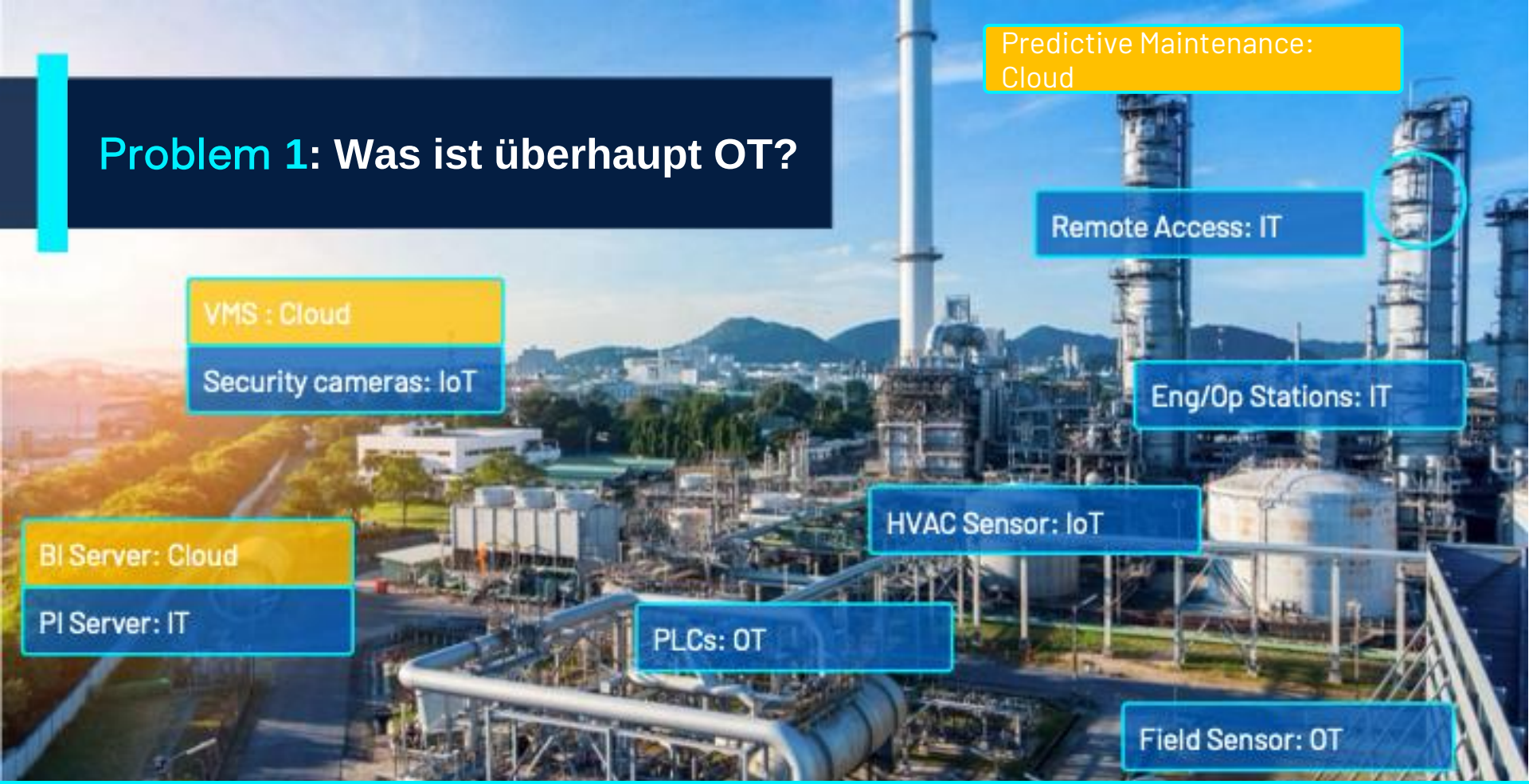
Vermeidbar
Vorfälle resultieren stets aus Fehlkonfigurationen, überbordenden Rechten und Schwachstellen.

Ausnutzbar
Risiken, die einfach zu erkennen und auszunutzen sind, vorallem aber “in the wild” ausgenutzt werden.

Impactful
Risiken für die Betriebs-stabilität, Umsatzgenerierung, Datensicherheit und –integrität

tenable

Problem 1: Was ist überhaupt OT?



Abhängigkeiten zu anderen Prozessen, z.B. ERP

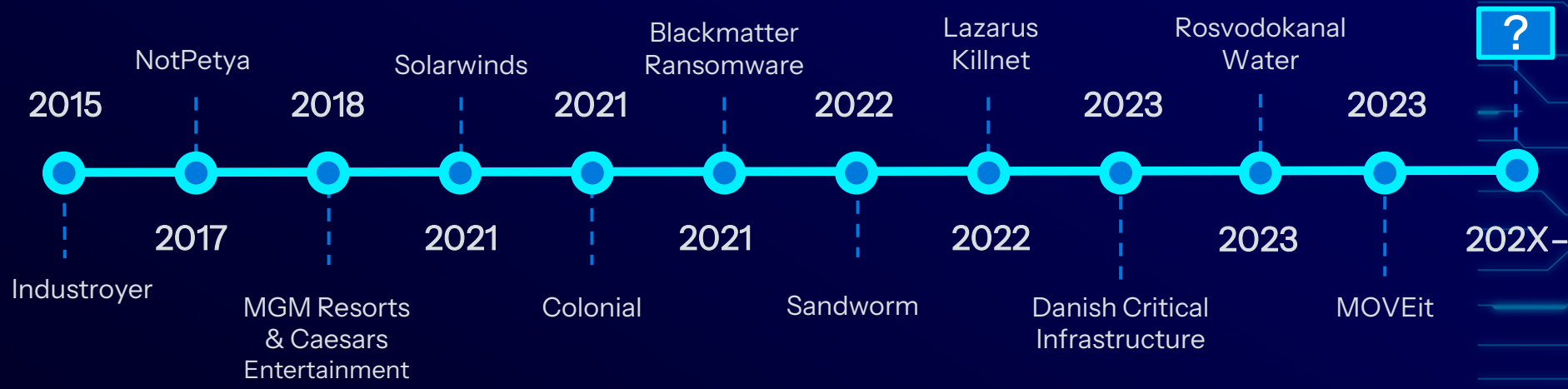
OT ist keine Asset-Klasse oder Gerätetyp.

OT ist die Antwort auf die Frage, wofür ein Asset genutzt wird.

Große Angriffswellen in den vergangenen Jahren

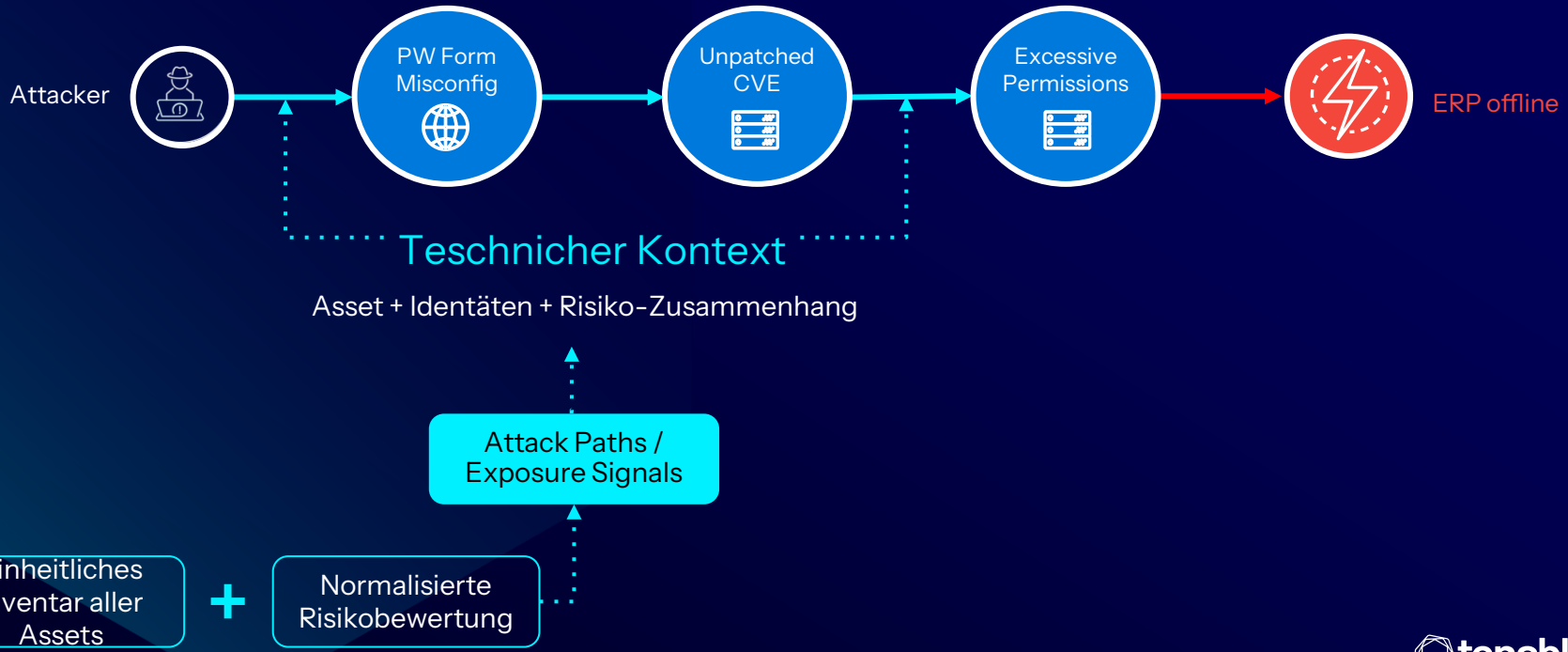
Wo liegen die Gemeinsamkeiten?

Verknüpfung mehrerer Technologien



tenable

Problem 2: Kein ausreichender technicher Kontext, um Exposure zu verstehen

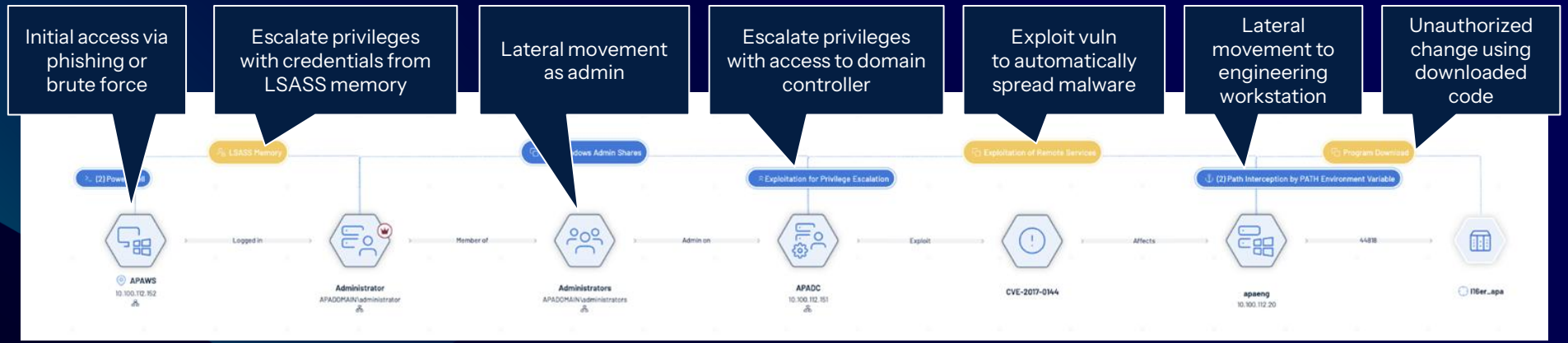


tenable

NotPetya: Über Identitäten und IT zur OT

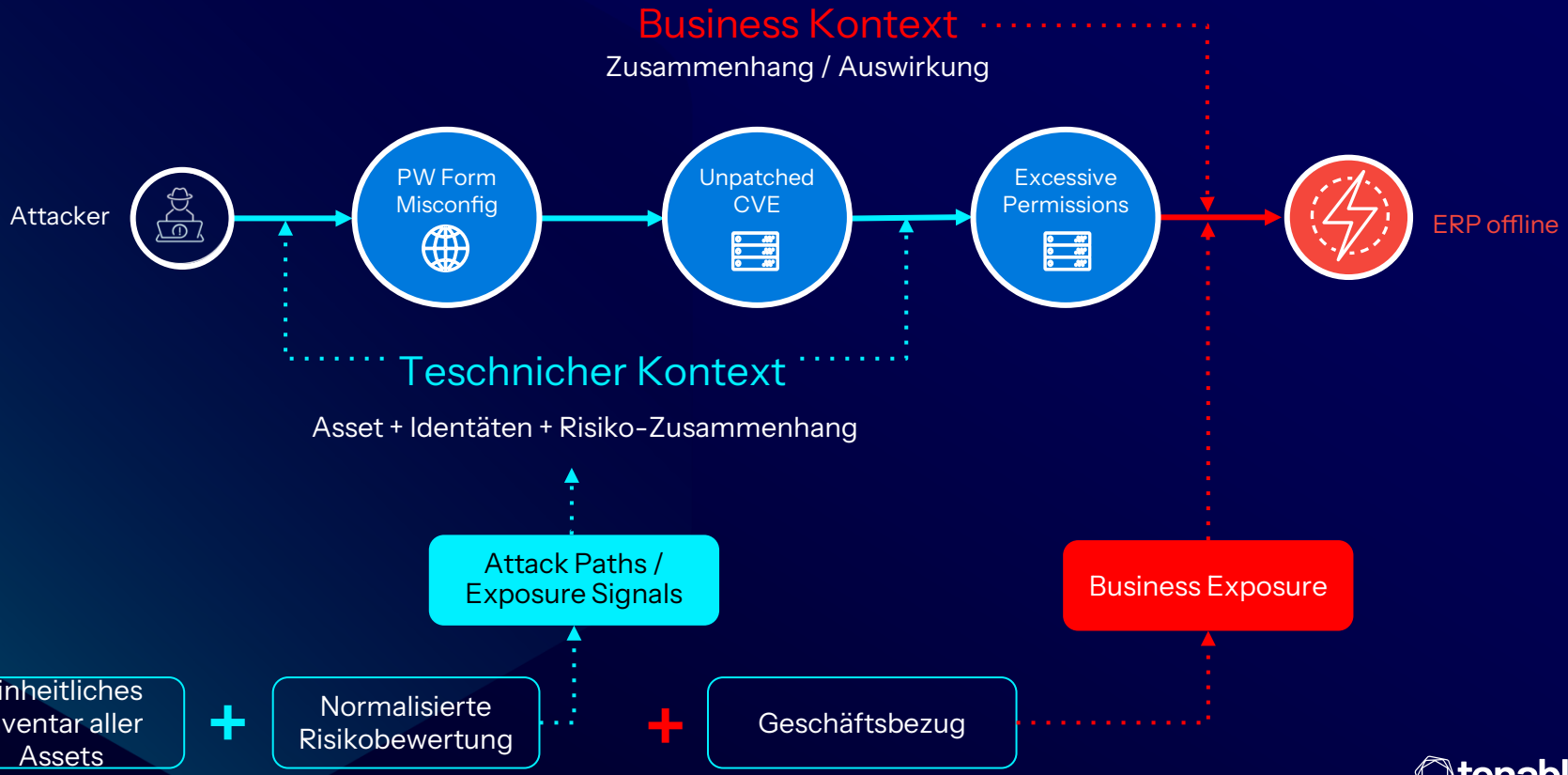
Geschätzter Schaden: $10 Milliarden
Typ: Malware
Einfluss: Betriebsunterbrechung, Datenverlust
Domains: OT, Identity, VM
Sponsor: Sandworm, GRU (Russland)

Erkenntnis:
Reine OT-Security-Produkte können solche Angriffe mangels Kontext zu Identitäten und IT nur zu spät erkennen und nicht verhindern.



tenable

Problem 3: Kein ausreichender Prozess-Kontext, um Exposure zu verstehen



Überwachungskameras…

… im Tresor

Vulnerabilities:
- ➔ 7 critical
- ➔ 5 medium
- ➔ 11 high

Der Kontext
ENTSCHEIDET

… in der Kantine

Vulnerabilities:
- ➔ 7 critical
- ➔ 5 medium
- ➔ 11 high

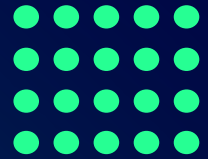
tenable

Technischen in betrieblichen Zusammenhang übersetzen

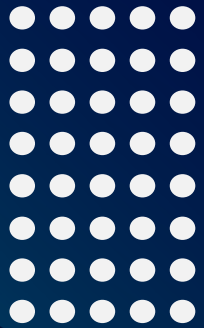
Aufdecken der **Angriffsfläche**

1

Identities



Assets

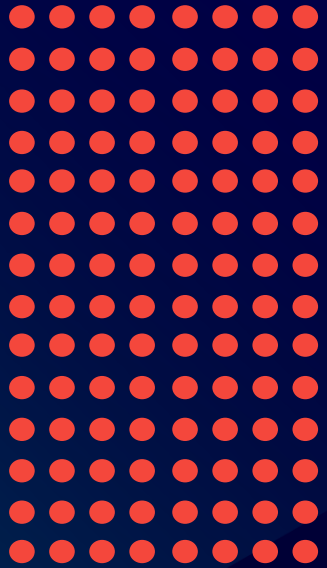


Identifikation aller Assets, intern, extern sowie Identitäten

Erkennen von **vermeidbare Risiken**

2

Vuln I Misconfig I Excess Permissions

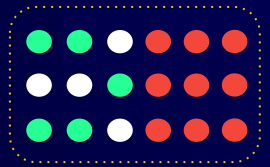


Technische Erhebung, jedoch unpriorisiert

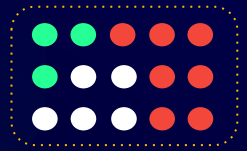
Darstellung des **Business Kontext**

3

Business Service A



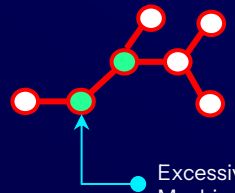
Business Process B

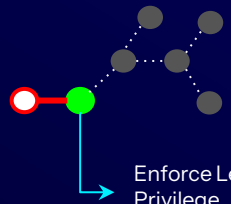


Verknüpfen von Assets, Identitäten, technischen Risiken und möglicher Auswirkungen auf den Betrieb

Beheben der **Exposure**

4

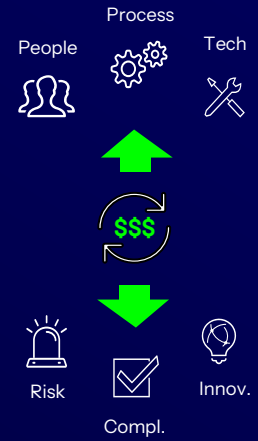




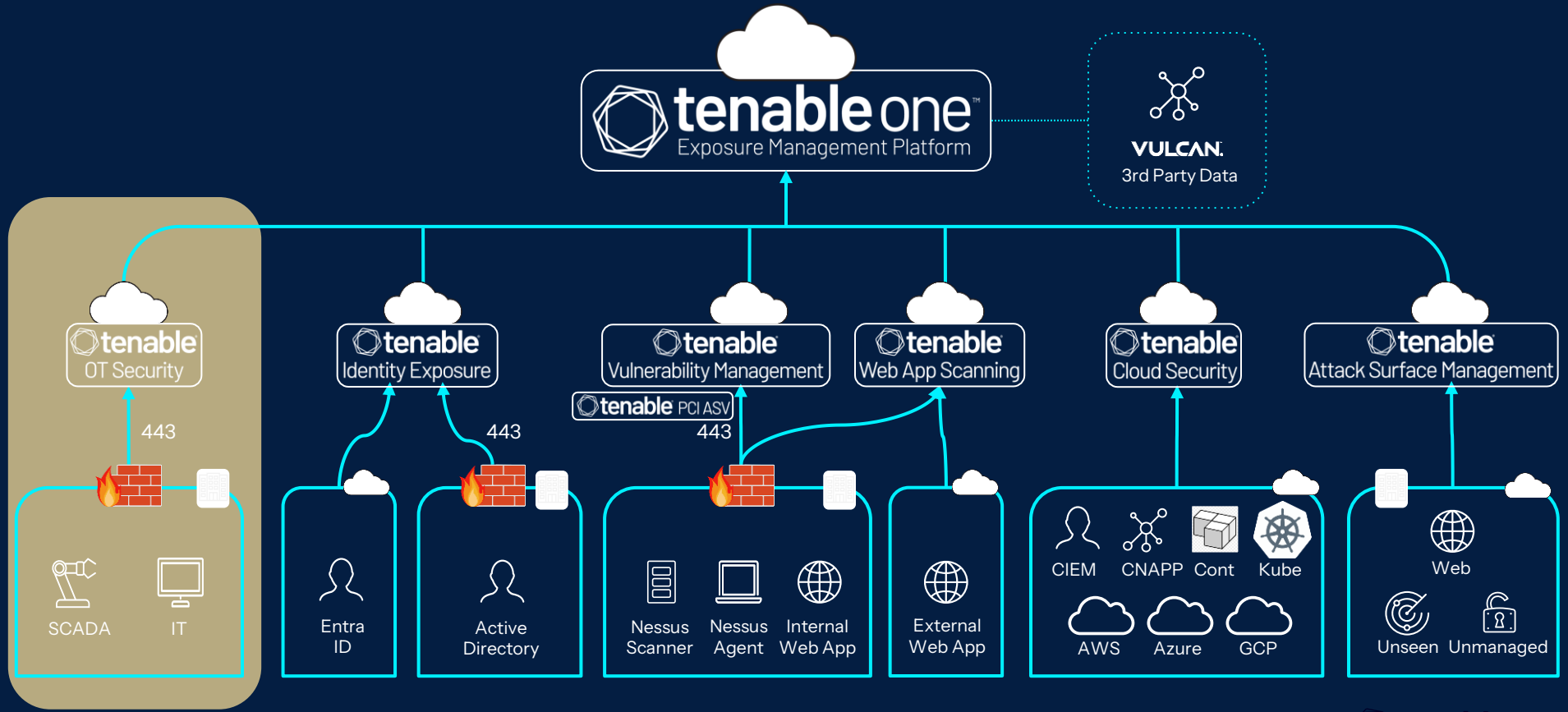
Angriffspfade untersuchen und Flaschenhals finden

Kontinuierliche **Prozessoptimierung**

5



tenable


tenable one
Exposure Management Platform
VULCAN.
3rd Party Data
tenable OT Security
tenable Identity Exposure
tenable Vulnerability Management
tenable PCI ASV
tenable Web App Scanning
tenable Cloud Security
tenable Attack Surface Management
443
443
443
SCADA
IT
Entra ID
Active Directory
Nessus Scanner
Nessus Agent
Internal Web App
External Web App
CIEM
CNAPP
Cont
Kube
AWS
Azure
GCP
Web
Unseen
Unmanaged

Nicht nur Security, sondern auch Safety

Tenable OT Security

Umfassendes, automatisiertes Asset-Inventar

Risikobasiertes Schwachstellen-management

Angriffs- und Anomalie-Erkennung

Erkennen und Verfolgen von Konfigurations-änderungen

HYBRID DISCOVERY

SECURITY MONITORING

tenable

Grundlagen schaffen: Was man nicht kennt, kann man nicht schützen

INPUTS

Tenable OT kann Daten aus diversen Quellen erheben und normalisieren

CSV files

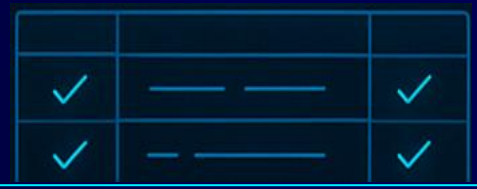
SCD files

IoT connectors

Third-party data

SNMP data

Sensors



tenable OT Security

Hybrid Discovery Engine

Aktive Abfragen
Herstellerspezifisch

Passives Monitoring

ERGEBNIS

Darstellung des Inventars, möglicher Angriffspfade und der Exposure, um priorisiert Abstellmaßnahmen zu treffen

Asset-Inventar

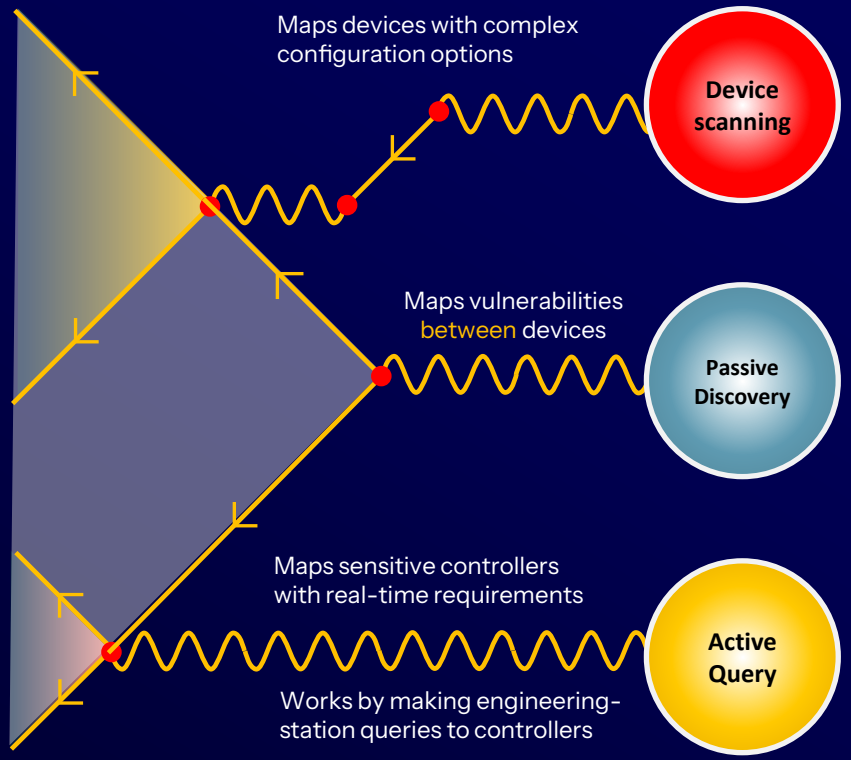
Angriffspfadanalyse

Exposure View

tenable

Hybrid Discovery

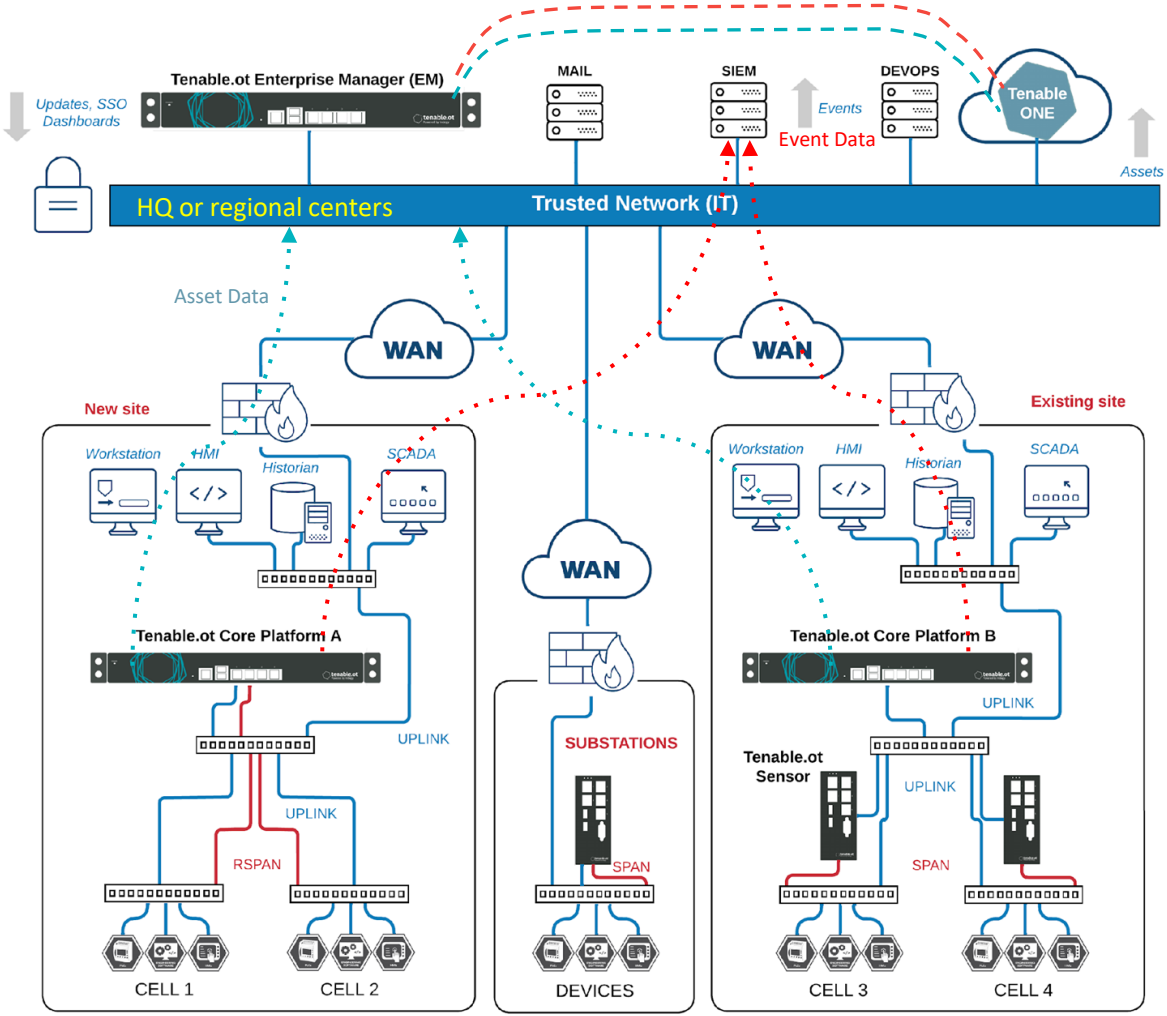
PURDUE	OPERATING SYS.
LEVEL 5 ENTERPRISE	WIN / LIN VM / SERVER
LEVEL 4 E.R.P.	WIN / LIN VM / SERVER
LEVEL 3 SITE OPERATIONS	WIN CLIENT ENGINEER STN
LEVEL 2 SUPERVISORY	EMBED. WIN/LIN HMI
LEVEL 1 CONTROL	RTOS / LINUX CONTROLLER/RTU
LEVEL 0 PHYSICAL PROCESS	EMBEDDED / NONE FIELD DEVICE



tenable

Tenable OT:

- OT Komponenten vollständig on-prem
- Exposure Management in der Cloud (Tenable One) verbunden über IT domain
- OT Discovery, VM und Security monitoring bleiben voll funktionsfähig ohne Cloud-Anbindung



Eine bessere Strategie ist gefragt

GEWÜNSCHTE ERGEBNISSE

Unterstützung des Business

Risikominderung

Optimierung von Kosten und Effizienz

Kommunikation und Automatisierung

Prioritäten I Workflow

Anreicherung durch Kontext

Technik I Business

Aggregation und Normalisierung

Assets I Risiken

- Fehlkonfigurationen
- Schwachstellen
- Übermäßige Berechtigungen

WACHSENDE ANGRIFFS-OBERFLÄCHE

AWS | Azure | GCP | Identitäten | Hybride Apps | OT/IoT | Private Cloud/IT

Gespräche mit Managern…

tenable

Gespräche mit Managern…

tenable


tenable

Controlware Vulnerability Management Service

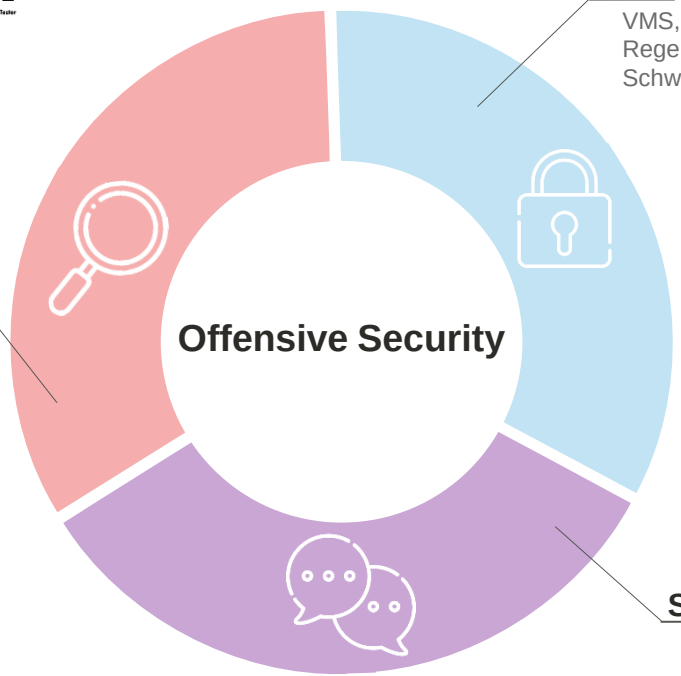
Ein ganzheitlicher Ansatz zur Absicherung komplexer IT- und OT-Infrastrukturen

Nils Rogmann, M.Sc.
Head of Competence Center Security

Dietzenbach, 02. Juli 2025

www.controlware.de

Competence Center Security | Offensive Security



Vulnerability & Exposure Management

VMS, EMS und External VMS
Regelmäßige und automatisiere Überwachung von Schwachstellen

Penetration Testing

Zielgerichtete Security-Assessments
Systematische Verwendung von fortgeschrittenen Angriffstechniken

Security Consulting

Kombination von Attack und Defense
Ganzheitliche Security-Betrachtung und -Beratung

Cyber Defense Service Portfolio

controlware

Controlware Cyber Defense Services

Managed Detection & Response (MDR)

- **SOC Core** – Basis EDR
- **SOC Complete** – Basis XDR
- **SOC Complete plus** – Basis XDR
- **SOC Cloud** – Basis CNAPP
- **VMS Light** (Basis Microsoft XDR)

Vulnerability & Exposure Management

- **VMS** (Vulnerability Management Service) – Tenable SC / VM
- **EMS** (Exposure Management Service) – Tenable One

Controlware Cyber Defense Assessments

- Compromise Assessment
- Vulnerability Assessment
- Penetration Testing & Red Teaming

Controlware Vulnerability Management – Was treibt uns an?

Die Frage ist nicht OB, sondern WANN ein Sicherheitsvorfall auftritt!

Herausforderungen

- Stetige Zunahme an Cyber-Kriminalität
- Angreifbare Systeme sind unbekannt
- Unzureichende Change- und Patch-Management-Prozesse

Auswirkungen

- Großteil der Angriffsoberfläche ist unbekannt
- Risiko eines erfolgreichen Cyber-Angriffs steigt

Unsere Empfehlungen

- Etablierung eines Vulnerability Managements
- Risiko systematisch identifizieren, analysieren und minimieren
- Angriffsoberfläche möglichst ganzheitlich sichtbar machen

7.2
Ø CVSS SCORE 2024

110
neue Schwachstellen pro Tag

Controlware Vulnerability Management – Überblick Service-Module

BUSINESS PROCESS
Erfassung & Priorisierung der Prozesse
Geschäftsprozessabhängige Risikobewertung
Benachrichtigung bei Business-Gefährdung

ASSET INVENTORY
Kontinuierliche Asset-Erfassung & -Inventarisierung
Identifizierung & Pflege von Verantwortlichkeiten

THREAT ADVISOR
Dedizierter Security Consultant
Regelmäßiger gemeinsamer Austausch
Bewertung & Priorisierung der Findings

SCAN & REMEDIATE
Regelmäßige Vulnerability Scans
Individualisierbare Untersuchungstiefe
Bewertung auf Basis von CVSSv3 & VPR

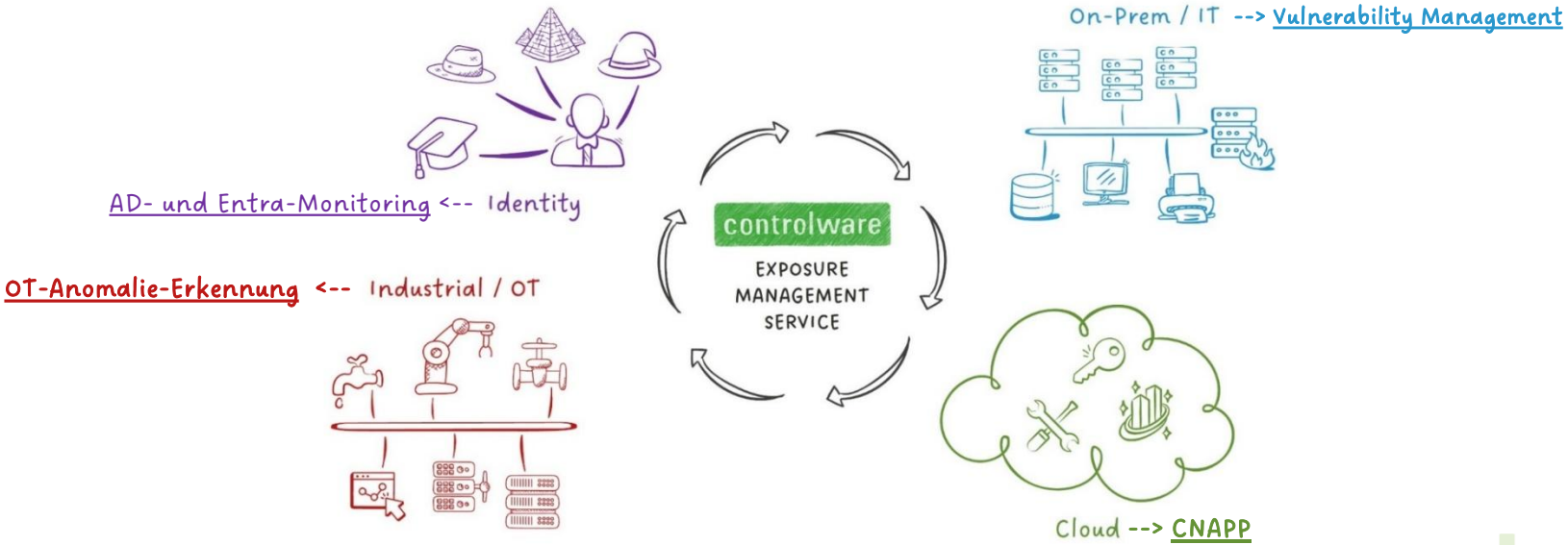
ON-DEMAND SCAN
Durchführung kurzfristiger Vulnerability Scans
bei veränderter Bedrohungslage

ALERT & REPORT
Zielgruppenorientierte Dashboards & Reports
Alarmierung bei kritischen Schwachstellen

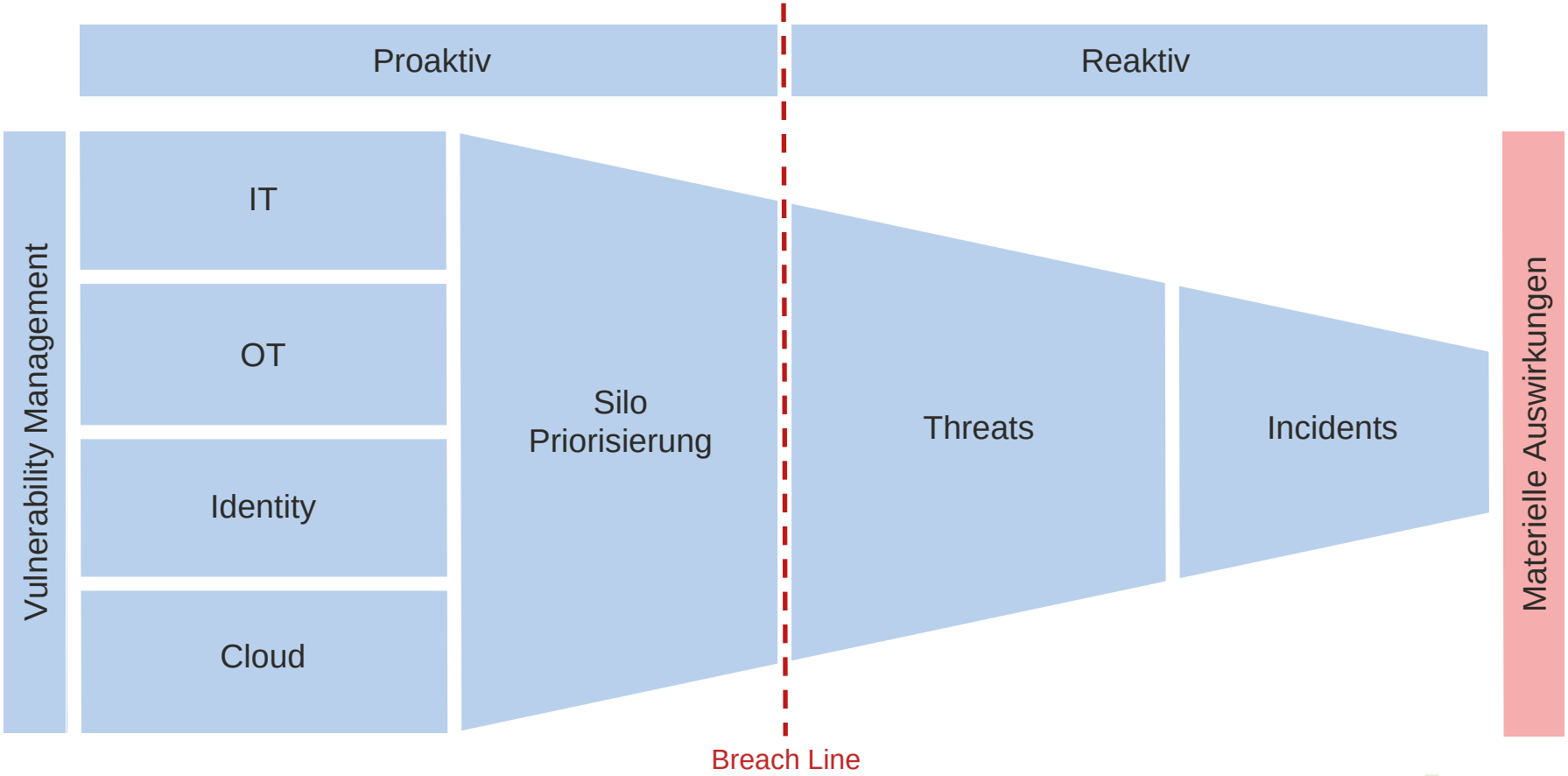
Exposure Management – Die moderne Angriffsoberfläche

Ganzheitlicher Lösungsansatz

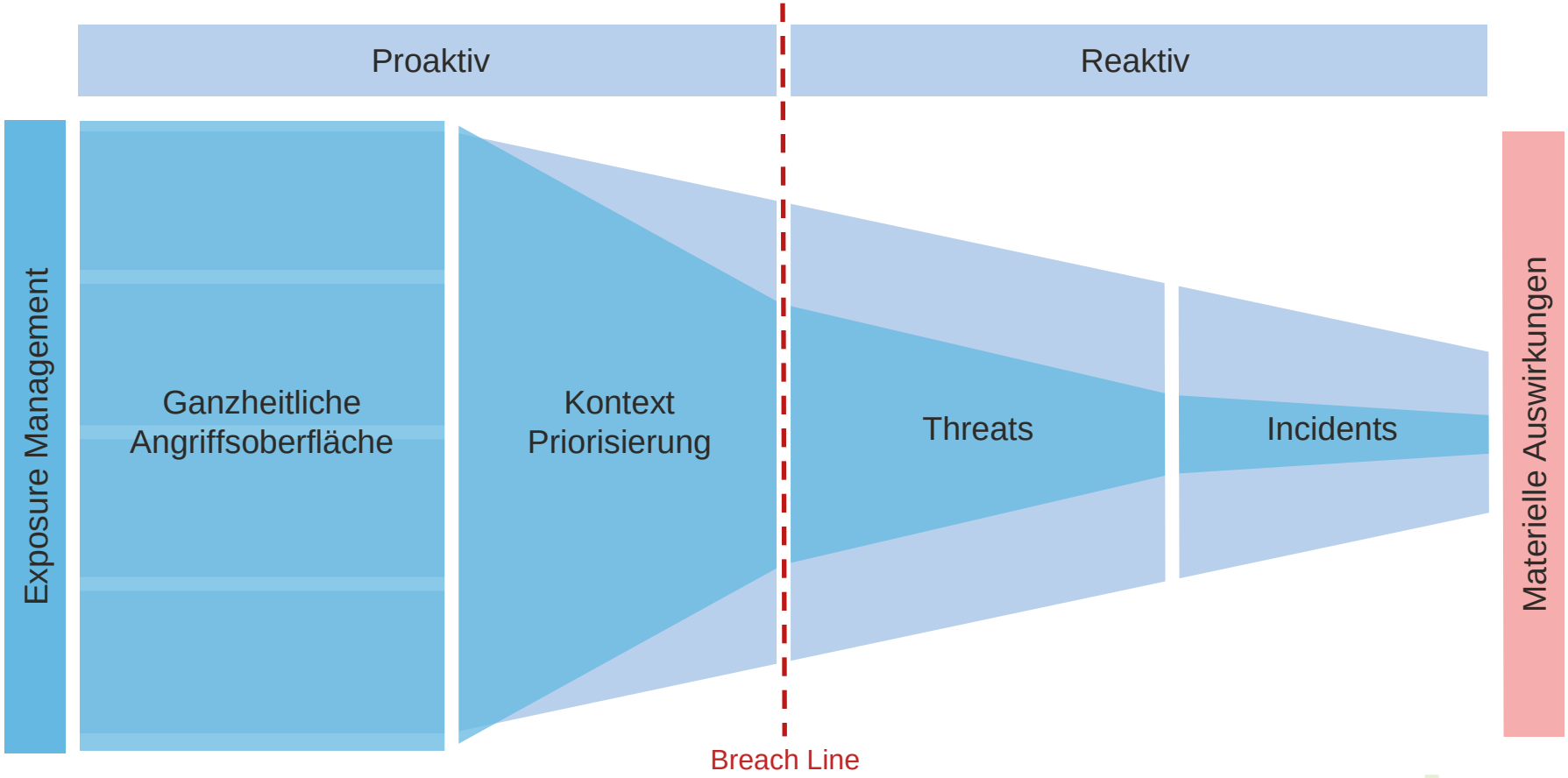
- Übergreifende Sichtbarkeit der Assets, Identitäten, Ressourcen und Schwachstellen
- Kontinuierliche Erfassung von Schwachstellen verschiedener Angriffsoberflächen
- Priorisierung und systematische Reduzierung von Risiken
- Identifizierung und Beseitigung konkreter Angriffspfade



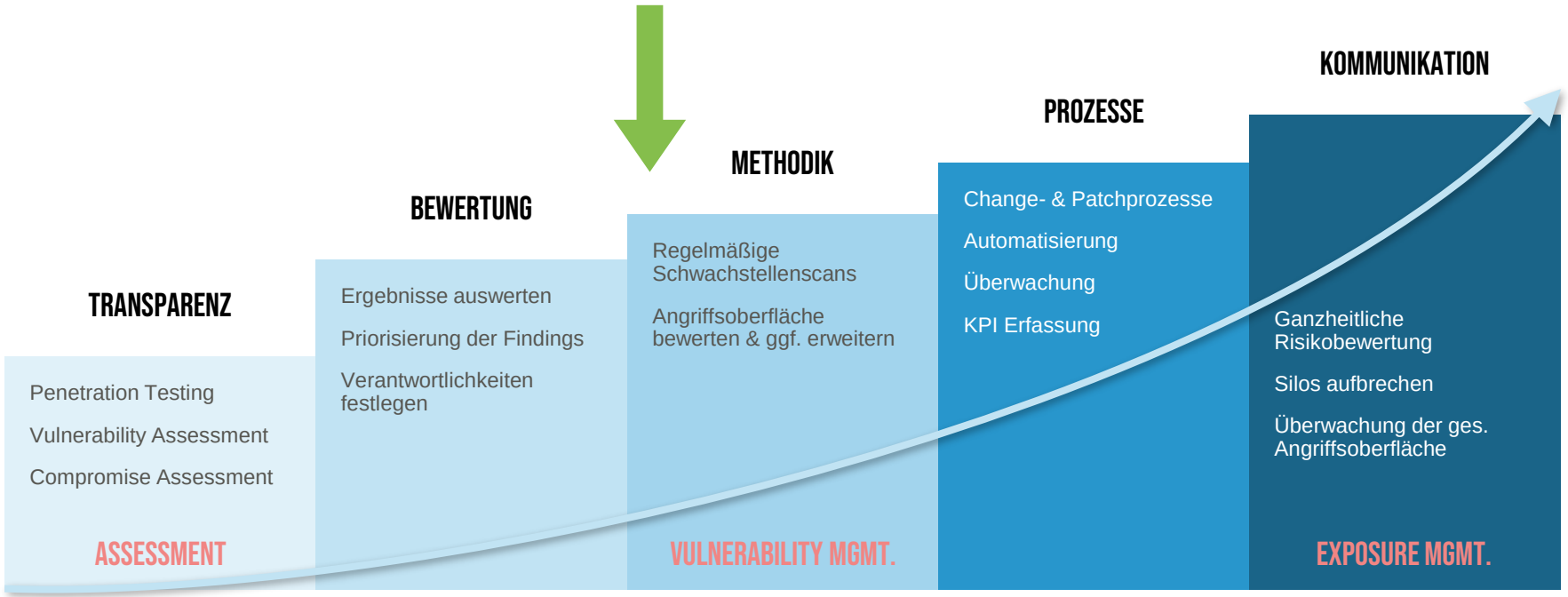
Vulnerability Management – Schwachstellen-Priorisierung



Exposure Management – Schwachstellen-Priorisierung



Standortbestimmung und Roadmap



SECURITY STRATEGIE DER NÄCHSTEN 3 BIS 5 JAHRE

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!

Nils Rogmann, M.Sc.
Head of Competence Center Security
Dietzenbach, 02. Juli 2025

www.controlware.de