Das Einmaleins des Exposure Managements

Durch Prävention Ihre Infrastruktur nachhaltig sicherer gestalten

Sabrina Fischer, Controlware

16.09.2025, Congress Park Hanau

Agenda

controlware

1. Was treibt uns an?
2. Wie schützen wir uns aktuell?
3. Warum sind wir noch nicht sicher?
4. Wie werden wir nachhaltig sicherer?
5. Was nehmen wir mit?

Was treibt uns an?

controlware

„Die Frage ist nicht **ob**, sondern **wann** ein Sicherheitsvorfall eintritt!“

Herausforderungen

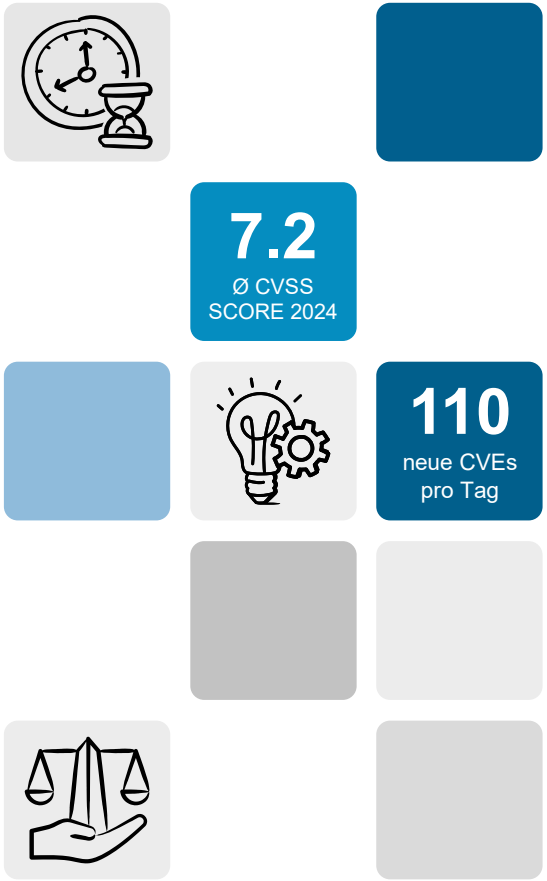
- Stetige Zunahme an Cyber-Kriminalität
- Angreifbare Systeme sind unbekannt
- Unzureichende Change- und Patch-Management-Prozesse

Auswirkungen

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

Unsere Empfehlungen

- Risiko systematisch identifizieren, analysieren und minimieren
- Etablierung eines Vulnerability Managements
- Weiterentwicklung zu einem **Exposure Management**



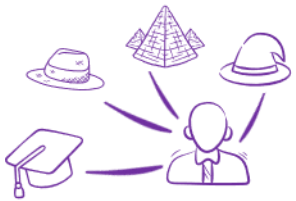
Wie schützen wir uns aktuell?

controlware

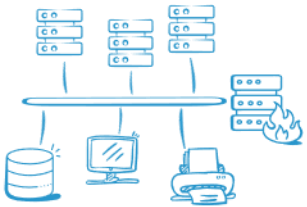
Exposure Management

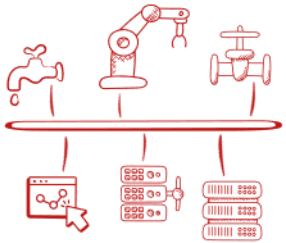
- Übergreifende Sichtbarkeit der Assets, Identitäten, Ressourcen und Schwachstellen
- Kontinuierliche Erfassung von Schwachstellen verschiedener Angriffsoberflächen
- Priorisierung und systematische Reduzierung von Risiken

AD- und Entra ID-Monitoring <--Identity



On-Prem / IT --> Vulnerability Management





OT-Anomalie-Erkennung <-- Industrial / OT

Cloud --> CNAPP

Wie schützen wir uns aktuell?

controlware

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
- Bewertungssysteme: CVSS & VPR

On-Demand Scans

- Durchführung kurzfristiger Vulnerability Scans bei veränderter Bedrohungslage

Alert & Report

- Zielgruppenorientierte Dashboards & Reports
- Alarmierung bei kritischen Schwachstellen

Warum sind wir noch nicht sicher?

controlware

Business Process

- Erfassung & Priorisierung der Prozesse
- Geschäftsprozessabhängige Risikobewertung
- Benachrichtigung bei Business-Gefährdung
- **„Silo“-Denken**
- **Limitierter Kontext**

Threat Advisor

- Dedizierter Security Consultant
- Regelmäßiger gemeinsamer Austausch
- Bewertung & Priorisierung der Findings

On-Demand Scans

- Durchführung kurzfristiger Vulnerability Scans bei veränderter Bedrohungslage

Asset Discovery

- Kontinuierliche Asset-Erfassung & -Inventarisierung
- Identifizierung & Pflege von Verantwortlichkeiten
- **Keine vollständige CMDB**
- **Keine vollständige Angriffsoberfläche**

Scan & Remediate

- Regelmäßige Vulnerability Scans
- Individualisierbare Untersuchungstiefe
- Bewertungssysteme: CVSS & VPR
- **Zu viele Schwachstellen**
- **Fehlende Priorisierung**
- **Zeit- / Fachkräftemangel**

Alert & Report

- Zielgruppenorientierte Dashboards & Reports
- Alarmierung bei kritischen Schwachstellen
- **Keine Verantwortlichen**
- **Keine festgelegten KPIs**

Wie werden wir nachhaltig sicherer? – Asset Inventory

controlware

Fragen zur Asset-Verwaltung

- Gibt es ein führendes System zur Netzdaten-Verwaltung?
- Wie regelmäßig wird das System aktualisiert?
- Existieren Prozesse / technische Lösungen zur Vermeidung von Schatten-IT?
- Können maliziöse Geräte innerhalb des Netzwerks detektiert werden?
- Welche Bereiche der Infrastruktur werden aktuell betrachtet?

Unsere Praxistipps

- Netzdaten im Schwachstellen Management-System regelmäßig (automatisiert) aktualisieren
- System-Verantwortlichen den Zugriff auf die Schwachstellen ermöglichen
- Gesamte Angriffsoberfläche betrachten (IT, OT, Cloud, Identity)

Wie werden wir nachhaltig sicherer? – Scan & Remediate

controlware

Systematische Identifizierung von Schwachstellen

- Wann erfolgte der letzte Schwachstellen-Scan?
- Welche Szenarien & Angriffspunkte wurden berücksichtigt?
- Welche Maßnahmen wurden aus den Ergebnissen abgeleitet?

Möglichkeiten zur Alarmierung

- In welchen Fällen soll eine Alarmierung erfolgen?
- Wer soll wann involviert werden?
- Welche Meldewege sind bereits im Unternehmen etabliert?

Unsere Praxistipps

- Regelmäßige Zielgruppen orientierte Schwachstellen-Reports
- Prozesse zur Nachverfolgung von Schwachstellen etablieren

Wie werden wir nachhaltig sicherer? – Scan & Remediate

controlware

Priorisierung von Findings

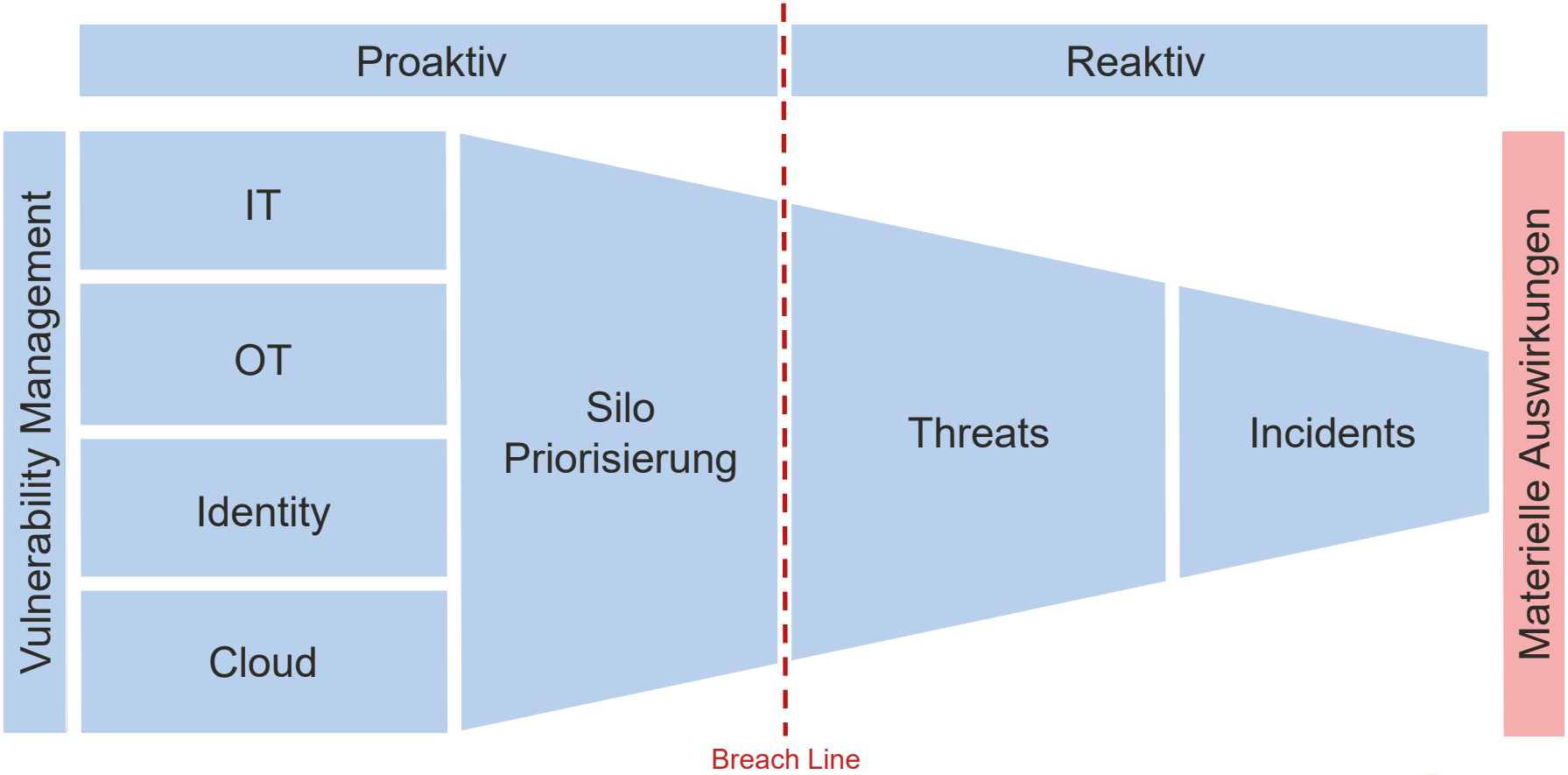
- Gibt es ein systematisches Vorgehen & klare Handlungsanweisungen zur Behebung von Findings (Kritikalität vs. „Quick-Wins“)?
- Woran liegt es wenn Schwachstellen nicht zeitnah geschlossen werden?
  - Fehlende Zeit / Ressourcen?
  - Vielzahl an identifizierten Findings?
  - Herausforderung bzgl. der Kommunikation?

Unsere Praxistipps

- Vernetzung innerhalb des Unternehmens
- Verantwortlichen Remediation-Scans ermöglichen
- Schwachstellen mit **Kontext** betrachten

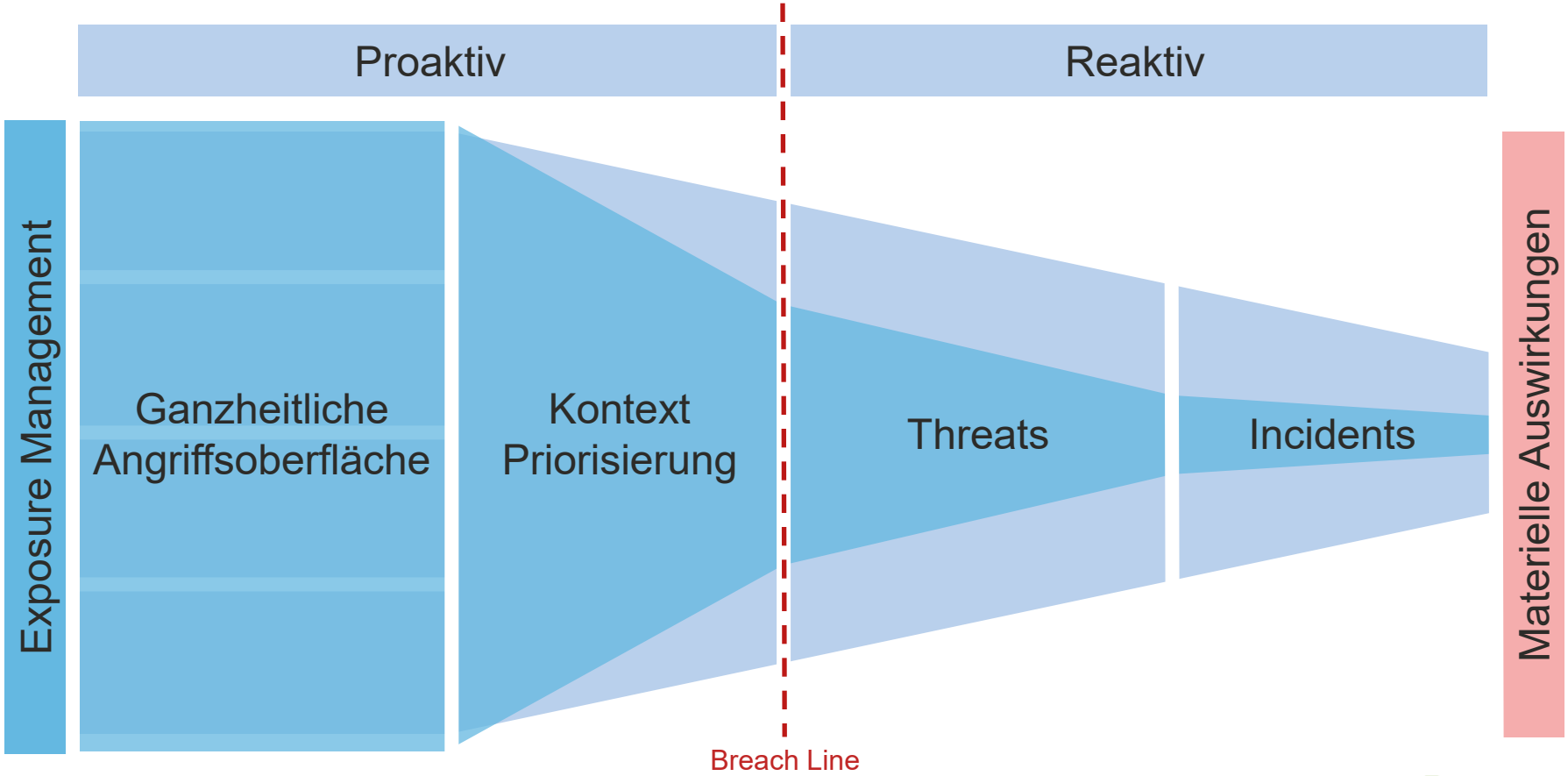
Wie werden wir nachhaltig sicherer? – Schwachstellen Priorisierung

controlware

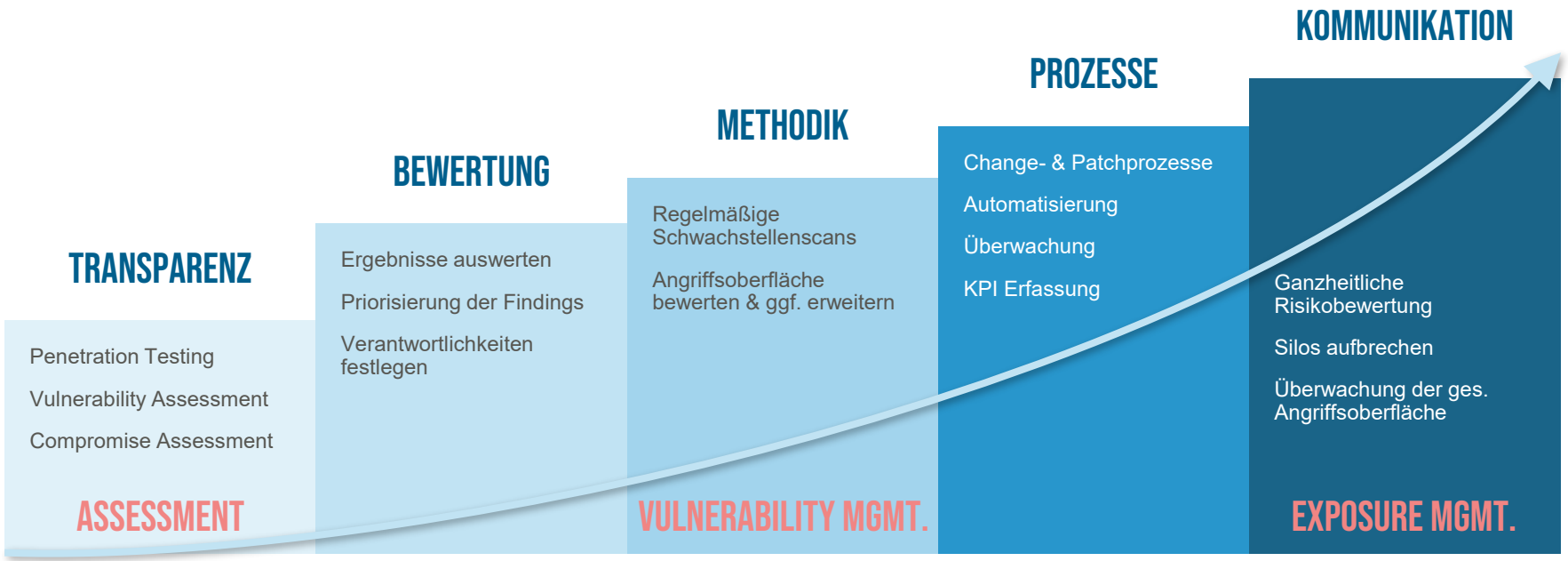


Wie werden wir nachhaltig sicherer? – Schwachstellen Priorisierung

controlware



Was nehmen wir mit?



SECURITY STRATEGIE DER NÄCHSTEN 3 BIS 5 JAHRE

Was nehmen wir mit?

controlware

Das Einmaleins des Exposure Managements

SILOS AUFBRECHEN

TRANSPARENZ SCHAFFEN

Gesamte Angriffsoberfläche betrachten

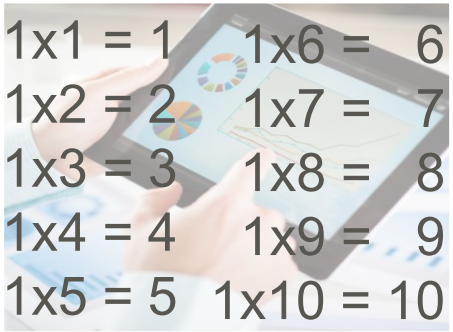
SCHWACHSTELLEN MITIGIERUNG

Methodik fürs Unternehmen entwickeln

KONTEXT

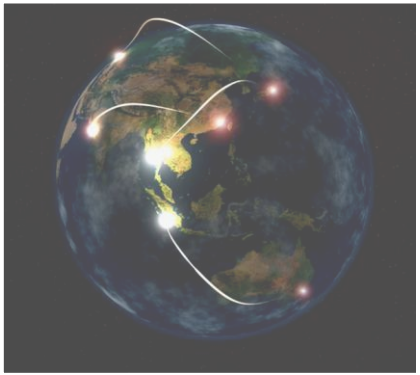
KPI DEFINITION

PROZESSE ETABLIEREN



Ganzheitliche Risikobetrachtung anstreben

KOMMUNIKATION



Controlware
Security Day

mailto: off-sec@controlware.de

Vielen Dank für Ihre Aufmerksamkeit!