

XM Cyber

Wie ein Continuous Threat Exposure Management (CTEM) ganzheitlich funktionieren kann

Tobi Traebing

Technical Director – EMEA

tobias@xmcyber.com

Der „Security Disconnect“

Eine isolierte
Wirklichkeit



IAM-Probleme



Alarmierungen



Schwachstellen

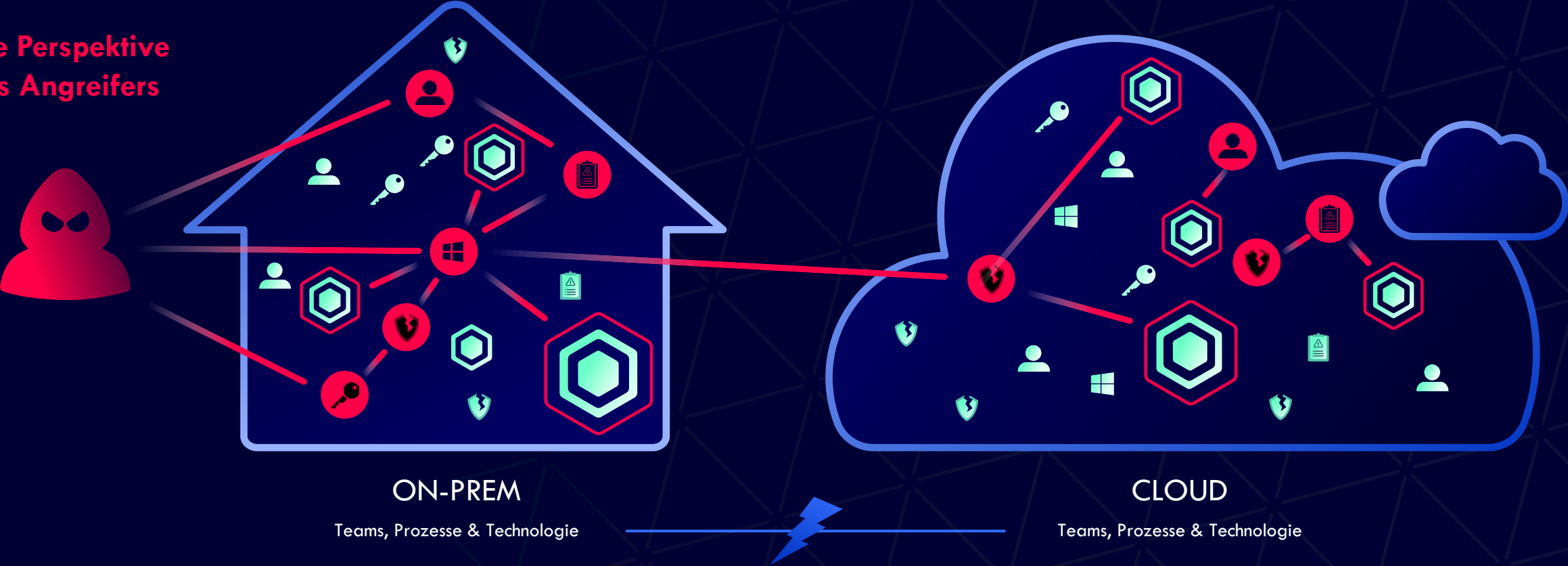


Lücken bei ext.
Anforderungen



Fehlkonfigurationen

Die Perspektive
des Angreifers



One By One is Never Done!

Im Durchschnitt
haben Organisationen

11'000

neue Risiken pro Monat

bis zu

250'000

Risiken in großen Unternehmen

Die Auswirkungen des „Security Disconnect“

Der derzeitige Ansatz funktioniert nicht

Was wir von unseren Kunden hören:

- Listen, die trotz Priorisierungstools nie enden
- Kostspielige, regelmäßige Pen-Tests
- Fehlende Abdeckung und keine einheitliche Sichtweise des Risikos
- Schlechte Kommunikation zwischen den IT- und Sicherheitsteams
- Fehlender Zusammenhang
- Wir werden immer noch angegriffen

Wir brauchen einen neuen Ansatz



Gartner's Continuous Threat Exposure Management (CTEM)

Gartner®

*“Establish regular **repeatable** cycles as part of your **continuous** threat exposure management program — guaranteeing consistent threat exposure management **outcomes**”*

75%

der Schwachstellen befinden sich nicht auf den Angriffswegen zu den kritischen Assets eines Unternehmens... dennoch konzentrieren sich die Unternehmen immer noch auf die Behebung dieser

2023 State of Exposure Management Report, XM Cyber

Ein neuer Ansatz ist notwendig

Entdecken Sie, wie ALLE Risiken zusammenkommen, sodass kritische Assets einem Risiko ausgesetzt sind



Konfigurationen



Zugänge



CVEs



Cloud



Active Directory

1. Discover & Prioritise

Discovery

Verability Assessment

In the Wild

RBVM: prioritize list by known or predicted (AI) exploitation

Exploitable Exposures

Nicht in der Lage, die Relevanz für Angreifer kontinuierlich zu überprüfen

2. Validate & Mobilise

75% Reduktion (Ausnutzbarkeit, Erreichbarkeit, Prüfung)

Ist es in meiner Umgebung ausnutzbar?

Critical Assets

Teil des Angriffspfad zum kritischen System?

90% weitere Reduktion

Choke Points

Teil mehrere Angriffspfade & Choke Point?

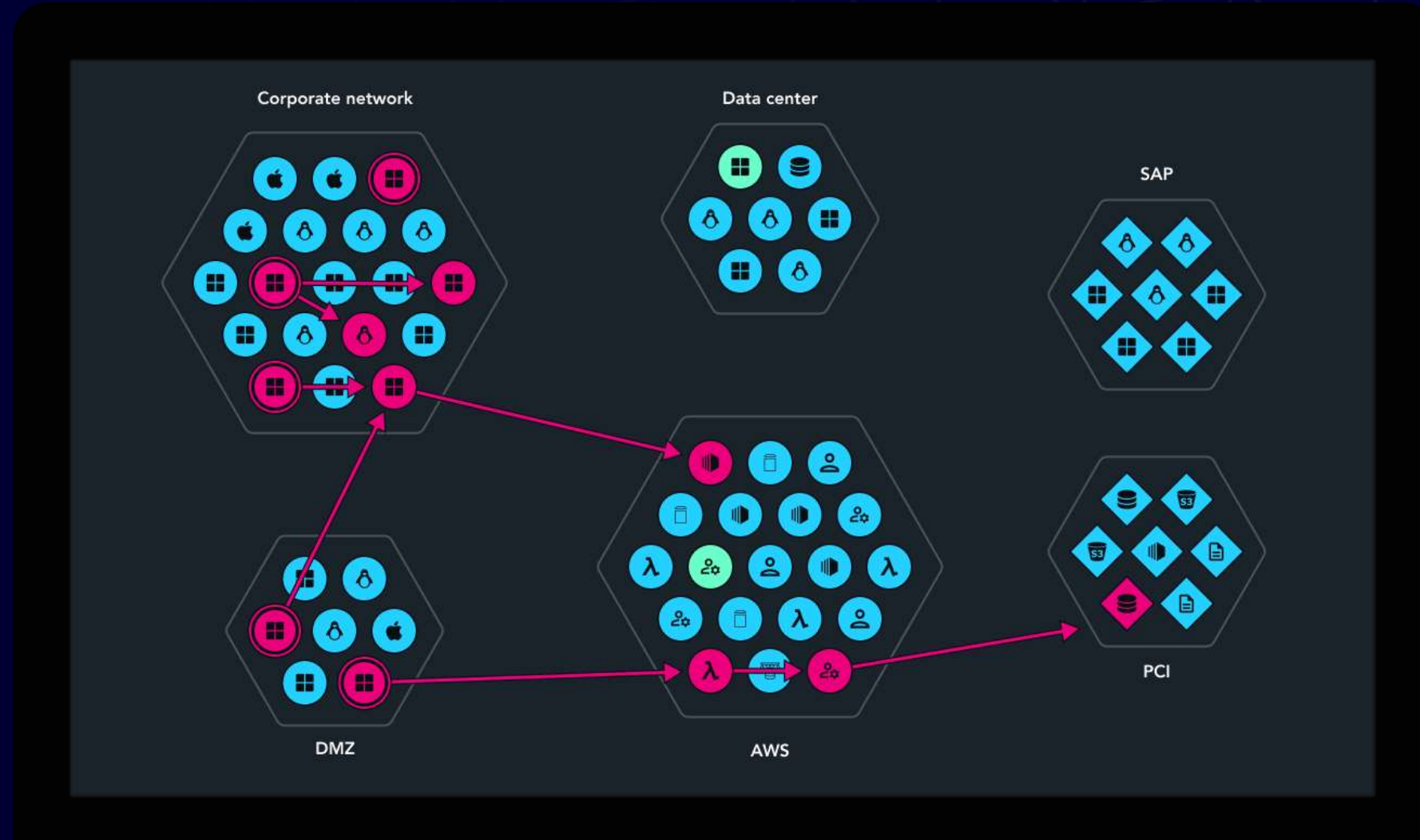
Von Angriffswegen zum Angriffsdiagramm

Alle Risiken ganzheitlich aufdecken

Eine einzige Ansicht über Ihre On-Premise- und Cloud-Netzwerke

Gezielte Verteilung der Ressourcen auf die Beseitigung von Gefahrenpunkten (Choke Points)

Härten Sie Ihre Umgebung, um die Gefährdung kontinuierlich zu reduzieren



Unternehmen können praktisch alle
Angriffswege zu kritischen Assets
eliminieren, in dem sie

nur 2%

der Schwachstellen beseitigen, die sich auf Choke Points
befinden.

2023 State of Exposure Management Report, XM Cyber

XM Cyber Continuous Exposure Management

Ermöglicht einen effizienten CTEM-Prozess



Attack Graph Analysis™

Kontinuierliche Analyse von Angriffstechniken in Kombination mit CVEs, Misconfigs, Identitätsrisiken usw.



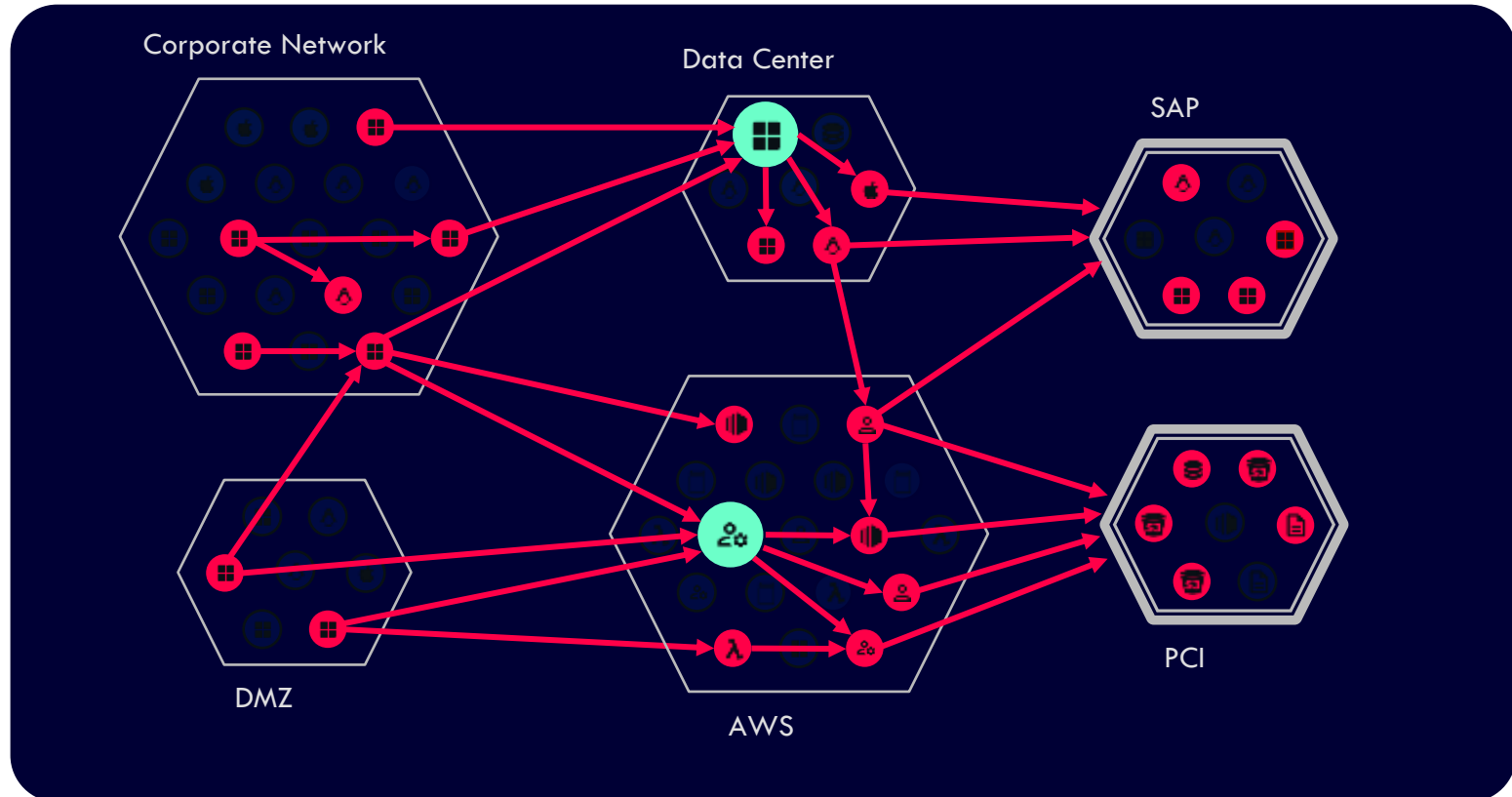
Validiert die Relevanz der Risiken und deckt Choke Points in hybriden Umgebungen auf



Sicheres Betreiben des Geschäftsbetriebs

Weniger beheben.

Mehr verhindern.



Halle 7
Stand 7-409

Vielen Dank!

 **XM Cyber** | See All Ways™