

Cleveres & wirtschaftliches Vulnerability  
Management mit XM Cyber

**VERSCHWENDEN  
SIE KEINE ZEIT (MEHR)!**

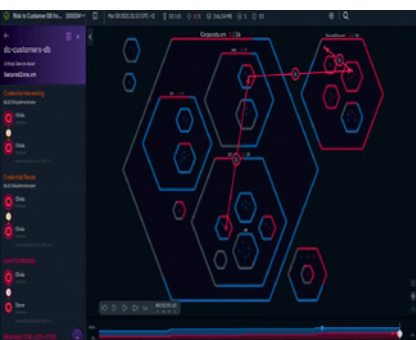
# AUF DIE RICHTIGEN MASSNAHMEN KOMMT ES AN – WIRTSCHAFTLICHKEIT UND SICHERHEIT SIND KEIN WIDERSPRUCH!

**75% der Sicherheitslücken liegen nicht auf Angriffspfaden, die zu kritischen Ressourcen führen.**

## FÜNF FRAGEN AN DAS SCHWACHSTELLENMANAGEMENT IHRER IT

1. Wissen Sie, wo die kritischen Informationen in den endlosen Listen von CVEs, Fehlkonfigurationen und Identitätsproblemen liegen?
2. Können Sie erkennen, wie einzelne Fehlkonfigurationen, Schwachstellen und unsicher verwaltete Anmeldedaten zusammenspielen?
3. Lassen sich Angriffspfade auf kritische Systeme und Daten durch das gesamte hybride Netzwerk identifizieren?
4. Sind Sie in der Lage, Risiken punktgenau einzuschätzen und die wirklich kritischen Schwachstellen zu benennen?
5. Sorgen Sie mit Ihren geplanten Maßnahmen für ein Maximum an Schutz und agieren dabei trotzdem wirtschaftlich?

**Falls Sie mindestens einmal Nein gesagt haben, ist es Zeit für einen neuen Ansatz: Continuous Exposure Management mit XM Cyber**



XM Cyber setzt Ihre Risiken in einen größeren Kontext. Sie können schneller entscheiden, welche Schwachstellen Sie bekämpfen sollten und welche zu vernachlässigen sind. Vergeuden Sie keine Zeit mehr mit Sicherheitslücken, von denen keine Angriffspfade zu kritischen Ressourcen ausgehen. Angriffsdiagramme zeigen Ihnen präzise die Engpässe, an denen Sie die Pläne von Hackern gezielt durchkreuzen können.

**Nur 2 % aller Schwachstellen beheben – und fast alle kritischen Angriffspfade abschneiden!**

## DER LEISTUNGSUMFANG IM ÜBERBLICK

- Identifizierung von Sackgassen und Engpässen
- Kontextbasierte Empfehlungen für Gegenmaßnahmen
- Sicherheits-Scores und -Trends
- Management von CVEs, Fehlkonfigurationen und Identitätsproblemen
- Active-Directory- und Identitätsschutz
- Sicherheitsmanagement für Hybrid-Cloud-Umgebungen

## DER FUNKTIONALE NUTZEN

- Keine toten Winkel – dank einer zentralen, umfassenden Übersicht, die alle relevanten Angriffswege im gesamten Hybrid-Netzwerk sichtbar macht
- Kein Rätselraten – da Analyse- und Modellierungstools detailliert zeigen, welche Wege ein Angreifer tatsächlich nehmen könnte
- Keine Unsicherheit – da die Tools ausführliche Anweisungen liefern, wie Sie die Wege der Angreifer Schritt für Schritt abschneiden können
- Keine Unterbrechungen – dank der automatisierten, fortlaufenden, sicheren und skalierbaren Lösung zur Risikominimierung in dynamischen Umgebungen

## DER WIRTSCHAFTLICHE NUTZEN

- Schwachstellenbehebung nur noch bei schädlichem Risiko
- Effektive Priorisierung & aussagekräftiges Risiko-Reporting
- Verhinderung von Angriffen durch proaktive Schließung von kritischen Sicherheitslücken
- Durchdachtes Zeitmanagement sorgt für weniger Arbeit und höheren Schutz

**Setzen Sie die richtigen Prioritäten! Machen Sie Ihre Mitarbeiter zu einem der wichtigsten Sicherheitsfaktoren! Kontaktieren Sie uns: [info@is4it.ch](mailto:info@is4it.ch)**