XM Cyber

Continuous Exposure Management-Plattform von XM Cyber

Angriffe verhindern, Unternehmensrisiken minimieren.

Hybride Unternehmensumgebungen werden laufend komplexer, und mit ihnen wächst die Zahl potenzieller Gefährdungen. Konventionelle Tools für Cybersicherheit melden Tausende Schwachstellen – doch können oft nicht die wenigen identifizieren, von denen eine tatsächliche Gefahr für geschäftskritische Ressourcen ausgeht. Verschiedenste Gefährdungen werden zusammengetragen, ohne dass die Lösungen ihre Ausnutzbarkeit, die Erreichbarkeit betroffener Ressourcen und die Wirksamkeit von Sicherheitskontrollen in Ihrer Umgebung evaluieren. So stehen Teams am Ende lediglich mit langen Listen irrelevanter Gefährdungen da und jagen den falschen Prioritäten nach. Gleichzeitig verkürzt agentenbasierte KI die Zeit, die Angreifer zum Ausnutzen von Schwächen brauchen, von Wochen auf Stunden. Sicherheitsteams können es sich also immer weniger leisten, Energie mit diesen irrelevanten Risiken zu vergeuden. Sie müssen Angriffswege kappen, bevor Kriminelle zuschlagen können.

XM Cyber bündelt relevante Gefährdungsarten fortlaufend in einem zentralen Angriffsdiagramm und zeigt Ihnen, wie Angreifer vorgehen könnten. Nach Analyse der potenziellen Angriffspfade zu Ihren kritischen Ressourcen erfolgt die Behebung der Schwachstellen, deren Ausnutzung ein echtes Risiko für Ihr Unternehmen wäre.

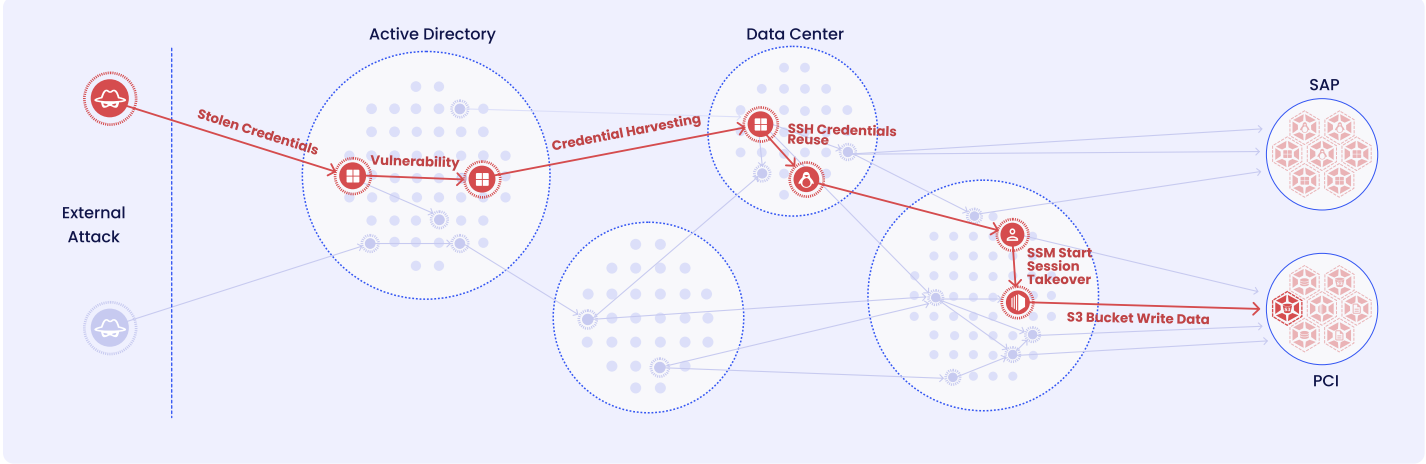
"XM Cyber klärt nicht einfach nur über die Zahl der Schwachstellen auf, sondern zeigt uns, wo Angreifer konkret ansetzen können. So können wir unsere IT-Teams präzise anleiten und müssen nicht mehr endlos über Prioritäten diskutieren – sondern setzen in Rekordzeit wirkungsvolle Schutzmaßnahmen um."
John Meakin, CISO, Equiniti

Nutzen

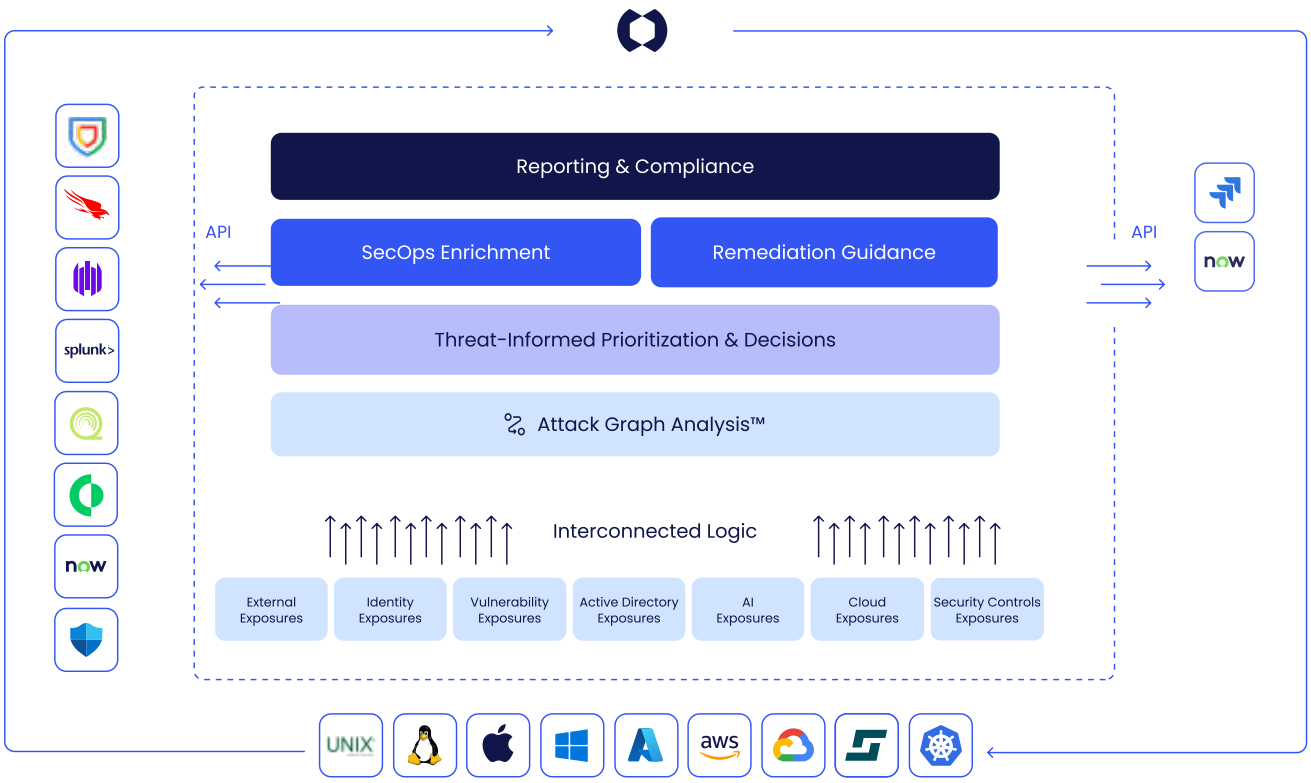
Identifizieren Sie sämtliche Gefährdungen und Pfade
Scannen Sie Ihre gesamte Angriffsfläche auf nachweisliche Gefahren und eliminieren Sie Angriffspfade, bevor Kriminelle sie ausnutzen können.

Priorisieren Sie nach tatsächlichen Auswirkungen
Fokussieren Sie Ihre Bemühungen auf sogenannte Choke Points – ausnutzbare Schwachstellen, an denen mehrere Angriffspfade zusammenlaufen. So steigern Sie die Effizienz Ihrer Schutzstrategie.

Belegen Sie Risiken und Dringlichkeit
Liefern Sie Teams und Entscheidern in der Führungsebene mehr Kontextinformationen und ermöglichen Sie koordinierte Maßnahmen, die Ihre Sicherheitslage nachweislich – und kostensparend – verbessern.



Continuous Exposure Management-Plattform von XM Cyber



Fortlaufendes Gefährdungsmanagement über die gesamte Angriffsfläche

XM Cyber operationalisiert ein durchgängiges Gefährdungsmanagement, das Schwachstellen, Fehlkonfigurationen, problematische Nutzeridentitäten und -berechtigungen, schwache Anmeldedaten, KI-basierte und weitere Gefährdungstypen miteinander zu validierten Angriffspfaden verknüpft. Von der externen Angriffsfläche bis zum internen Netzwerk, am Unternehmensstandort genau wie in Multi-Cloud-Umgebungen.

Validierung echter Gefährdungen – ohne „Hintergrundrauschen“

XM Cyber erstellt einen digitalen Zwilling Ihrer gesamten Umgebung, um verschiedenste Ausnutzbarkeits- und Zugangsbedingungen für jede Schwachstelle zu testen, wobei aktive Sicherheitskontrollen in Ihrer Umgebung berücksichtigt werden.

Aussagekräftiges Reporting zu Risiken und Compliance

XM Cyber reduziert nicht nur deutlich das Risiko für geschäftskritische Prozesse und Ressourcen, sondern unterstützt Sie auch dabei, die erzielten Verbesserungen effektiv an Ihre Unternehmensführung zu kommunizieren. Dank fortlaufender Überwachung von Assets und Sicherheitskontrollen auf Richtlinienverstöße sind Audits jederzeit möglich.

Geschäftsorientierte Priorisierung und Umsetzung von Schutzmaßnahmen

XM Cyber priorisiert Abhilfemaßnahmen im weiteren Kontext ihrer geschäftlichen Auswirkungen: Die Schwachstellen, die die größte Anzahl kritischer Ressourcen gefährden und sich an Schnittpunkten mehrerer Angriffspfade (Choke Points) befinden, haben höchste Priorität. So können mit einer einzigen Korrektur viele Angriffspfade beseitigt werden.

“XM Cyber hat uns dabei geholfen, aus Tausenden kritischen Schwachstellen die relevanten Fixes herauszufiltern – und unser Gefährdungsniveau von 98 % auf 2 % zu reduzieren. Für uns ist das ein echter Game-Changer.”
Ilaria Buonagurio, Leiterin CIS-Prävention, Globaler Einzelhändler für Luxusartikel

XM Cyber