Managed Exposure Defence: Ein Programm für die gesamte Response-Schleife

Herausforderung für Unternehmen

Im April 2026 setzte Anthropic's Project Glasswing ein hochmodernes KI-Modell ein, trainierte und testete es, um kritische Schwachstellen zu finden. Dies führte zur Entdeckung von Tausenden bisher unbekannter Fehler in allen großen Betriebssystemen und Browsern – einige waren jahrzehntelang unentdeckt. Anbieter arbeiten nun unter Hochdruck an kontrollierten Patches nach einem Offenlegungsplan, was eine koordinierte Patch-Welle auslöst, wie sie die Branche noch nie erlebt hat.

Für die meisten Organisationen ist die Herausforderung nicht das Wissen darüber, sondern die eigenen Kapazitäten. KI-gestützte Exploit-Entwicklung hat das Fenster von der Offenlegung zur Waffe von Tagen auf Stunden verkürzt. Sicherheitsteams sind bereits überlastet, ohne dedizierte Patch-Operations-Funktion und ohne Reservekapazitäten. Regulierungsbehörden erwarten eine nachweisbare Reaktion auf ein bekanntes Ereignis. Vorstände stellen bereits Fragen. Und die Bedrohung kann nicht auf lange Beschaffungszyklen oder fragmentierte Vendor-Beziehungen warten.

Unsere Lösung

Insight Managed Exposure Defence ist ein gebündelter Managed Service, speziell für diesen Moment konzipiert – mit fünf integrierten Fähigkeiten in einem einzigen Programm, das Organisationen von der Gefährdung zur geschützten Umgebung mit der Geschwindigkeit bewegt, die die Bedrohung erfordert. Statt fragmentierte Point-Tools und separate Anbieter zu koordinieren, erhalten Organisationen eine durchgehende Abdeckung der gesamten Vulnerability-Response-Schleife mit einheitlicher Verantwortung.

Das Programm kann innerhalb von 24 Stunden nach dem ersten Kontakt umfang- und preisgerecht definiert werden und skaliert von 100 verwalteten Assets bis zur großen Enterprise-Größe ohne benutzerdefinierte Entwicklung – und bietet sofortige operative Entlastung unabhängig von der Organisationsgröße.

Features & Vorteile

Ein Vertrag. Ein Team. Eine Antwort.

Insight deckt alle fünf Phasen der Response-Schleife mit einem einzigen Delivery-Team ab. Keine Verantwortungslücken zwischen Anbietern. Kein Koordinationsaufwand.

Ergebnis: Umfang und Preis innerhalb von 24 Stunden

Von der ersten Gespräch zur geschützten Umgebung – ohne die langen Beschaffungszyklen, auf die die Bedrohung nicht warten kann.

Skaliert von 100 Assets bis Enterprise

Out-of-the-Box-Bereitstellung in jeder Größe – keine benutzerdefinierte Entwicklung erforderlich, keine minimale Engagement-Komplexität.

Compliance-ready by Design

Ausgerichtet auf große Regulierungsrahmen wie NIS2, DORA, GDPR usw. Audit-Trail ist von Tag eins integriert.

Outcome

Mit Insight Managed Exposure Defence verschiebt sich die Denkweise von „Wie reagieren wir?" zu „Es ist bereits geregelt." Organisationen erhalten sofortige operative Entlastung von einer Bedrohung, die ihre interne Kapazität übersteigt, eine nachweisbare Sicherheitslage, die Regulierungsbehörden und Vorstände zufriedenstellt, und das Vertrauen, dass ein einziger Partner die gesamte Response übernimmt.

Fünf Phasen. Eine Insight.

Unser Unterschiedungsmerkmal: alle Services aus EINER Hand.

Wir liefern in jeder Phase der Response-Schleife: Exposure-Erkennung, Sichtbarkeit der Software-Supply-Chain, betriebsseitige Behebung, Code-seitige Behebung und Exploit-Erkennung und Eindämmung – alles auf einem einzigen Vertrag mit einem einheitlichen Delivery-Team.

Managed CTEM

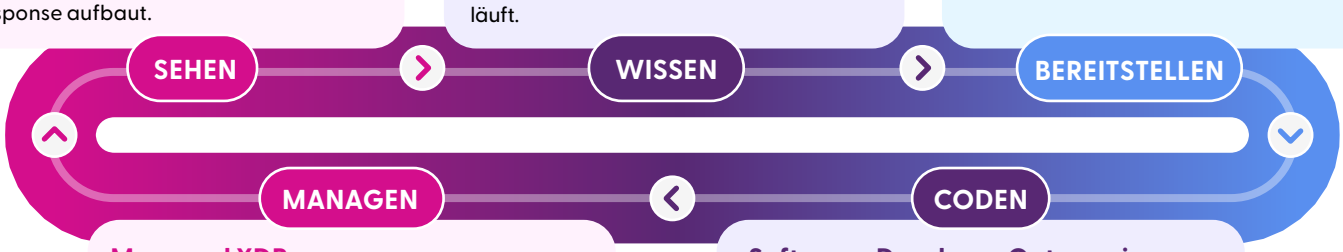
Kontinuierliches Scanning über Endpoints, Cloud, Identität und Anwendungen – mit einer Echtzeit-, risiko-bewerteten Exposure-Karte. Das Fundament, auf dem die gesamte Response aufbaut.

Software-Supply-Chain & OSS-Risiko

SBOM-Generierung, Open-Source-Dependency-Überwachung und Überprüfung der Vendor-Vertragsposition. Sichtbarkeit in das, was in Ihren Systemen läuft.

Managed patch

Enterprise-Scale-Patch-Operationen über Windows®, Linux®, Hypervisoren und die Datenbankebene. Change-managed Bereitstellung mit Test-Ringen, Rollback und zeitgestempeltem Audit-Trail.



Managed XDR

24/7/365 Erkennung, Triage und Response von einem globalen SOC in den USA, UK, Indien und Manila. Das Sicherheitsnetz, wenn Patches verzögert werden.

Software-Developer Outsourcing

Surge-Engineering-Kapazität für Dependency-Upgrades, Library-Refactorings und benutzerdefinierte Anwendungs-Behebung. Exposure auf Code-Ebene geschlossen, ohne Ihre Produkt-Roadmap einzufrieren.

Möchten Sie noch weiter gehen?

GRC Assessment

Evaluieren Sie die Governance-, Risiko- und Compliance-Postur Ihrer Organisation über große Industrie-Frameworks hinweg, identifizieren Sie Lücken und bauen Sie einen klaren Weg zur Audit-Bereitschaft auf.

Penetration Testing & Continuous Pen Testing

Erreichen Sie proaktive Validierung Ihrer Sicherheitslage durch simulierte Angriffsszenarios – und bestätigen Sie, dass Patches und Kontrollen wie beabsichtigt funktionieren.

Managed AI Governance

Ermöglicht Organisationen, KI verantwortungsvoll zu skalieren, indem kontinuierliche Sichtbarkeit, Governance-Insights und umsetzbare Empfehlungen über Nutzung, Agenten, Identitäten und Kosten bereitgestellt werden.

Warum Insight?

Insight Enterprises ist ein führender Solutions Integrator, der Kunden hilft, Technologie-Herausforderungen zu lösen, indem die richtige Hardware, Software und Services kombiniert werden. Als Fortune-500-Technologieunternehmen, gestützt auf 35+ Jahre Expertise und ein tiefes Netzwerk von 6.000+ Partnern, liefern wir sichere, durchgehende IT-Lösungen für Organisationen weltweit.