HADRIAN

Wie Exposure-Management unentdeckte Risiken reduziert

Eine moderne Lösung zum Schutz der wichtigsten Vermögenswerte und Assets von Organisationen.

Die äußere Grenze der externen Angriffs Oberfläche ist nicht mehr definiert

Vermögenswerte und Assets existieren am Perimeter mehr als jemals zuvor

In der schnelllebigen Welt von heute sind Unternehmen gezwungen, die digitale Transformation anzunehmen, um wettbewerbsfähig zu bleiben. Die Vorteile der digitalen Transformation sind bedeutend und weitreichend.

- **Verbesserung der Kundenerfahrung** – Durch die Nutzung von Technologien wie mobilen Apps, sozialen Netzwerken und Chatbots können Unternehmen personalisierte Interaktionen mit ihren Kunden schaffen.
- **Steigerung der Effizienz und Produktivität** – Digitale Werkzeuge haben manuelle Prozesse automatisiert, Fehler reduziert und die Genauigkeit verbessert. Dies gibt Mitarbeitern die Freiheit, sich auf Aufgaben mit höherem Mehrwert wie Innovation und Geschäftsentwicklung zu konzentrieren.
- **Größere Agilität und Flexibilität** – Cloud-basierte On-Demand-Anwendungen haben Organisationen geholfen, ihre Operationen schnell zu skalieren, sowohl nach oben als auch nach unten. Und, Fernarbeitstools ermöglichen es Mitarbeitern, effizienter zu arbeiten.

Indem sie die digitale Transformation angenommen haben, konnten Organisationen der Kurve voraus bleiben, sich an verändernde Marktbedingungen anpassen und aufkommende Möglichkeiten nutzen. Allerdings haben die Aktivitäten der digitalen Transformation den Sicherheitsperimeter von Organisationen verwischt. Mit mehr Mitarbeitern, Kunden und Drittanbieteranwendungen, die auf die Unternehmensinfrastruktur zugreifen, ist das Risikomanagement zunehmend schwieriger geworden.

40%

der Unternehmen werden bis 2023 eine Cloud-native Strategie als Priorität verfolgen, um Agilität und Effizienz zu steigern und gleichzeitig Kosten zu senken, laut der Cloud-Infrastrukturumfrage von Forrester aus dem Jahr 2022.

24%

mehr Arbeitnehmer haben sich 2022 im Vergleich zu 2021 für Fernarbeit entschieden.

87%

der Führungskräfte haben laut Gartner im Jahr 2021 die digitale Transformation als eine Hauptpriorität für ihre Organisation identifiziert.

Bedrohungsakteure nutzen die neue Grenze

Angriffe zielen zunehmend auf exponierte Vermögenswerte ab

Die digitale Transformation bringt auch neue Risiken und Herausforderungen mit sich, insbesondere in Bezug auf die Cybersicherheit. Cyberkriminelle und Bedrohungsakteure nutzen schnell die Schwachstellen in der digitalen Infrastruktur aus, was zu Datenverletzungen, finanziellen Verlusten und Reputationsschäden für Organisationen führt.

Im Eifer, neue Technologien zu adoptieren und der Konkurrenz voraus zu sein, werden Sicherheitsüberlegungen oft vernachlässigt. Cloud-Computing, IoT-Geräte und mobile Anwendungen, unter anderem, haben zu einer erweiterten Angriffsfläche geführt, die von Bedrohungsakteuren ausgenutzt werden kann.

> “
>
> Es besteht die Wahrnehmung, dass Organisationen ihre Sicherheitsbemühungen um ihre traditionellen „bekannten“ Umgebungen konzentrieren. Dies schafft einen Anreiz für Bedrohungsakteure, da sie eher ein im Internet exponiertes Asset finden können, das sie ausnutzen können.
>
> **Olivier Beg - Leiter des Hackings bei Hadrian**

Organisationen sollten sich auf die Vorteile der digitalen Transformation konzentrieren und die Risiken und Bedrohungen, die damit einhergehen, adressieren. Bedrohungsakteure nutzen diesen Mangel an Sicherheitsüberlegungen aus, indem sie die Schwachstellen in neuen Technologien gezielt angreifen und ausnutzen, um auf sensible Daten zuzugreifen.

69%

der Organisationen wurden von einem Angriff getroffen, der ein unbekanntes, schlecht verwaltetes oder unzureichend verwaltetes externes Asset zum Ziel hatte.

10/55

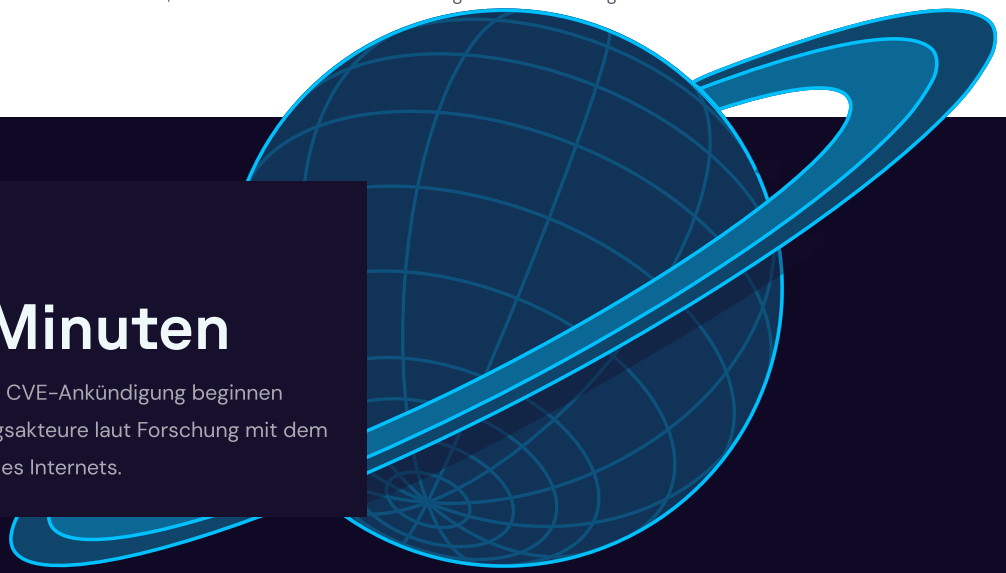
der im Jahr 2022 ausgenutzten Zero-Day-Schwachstellen betrafen Geräte am Rande des Internets.

Wie die Bedrohungslandschaft umgestaltet wird

Anfangszugangsbroker haben ganz andere Anreize als traditionelle Bedrohungsakteure

Anfangszugangsbroker (Initial Access Brokers, IAB) sind Teil eines wachsenden Trends zur Zusammenarbeit in der kriminellen Welt. Historisch gesehen haben Ransomware-Banden und andere Bedrohungsakteure alle Aspekte eines Angriffs selbst durchgeführt, von der Erlangung des Zugangs zu einem Netzwerk über die Verschlüsselung von Daten bis hin zur Verhandlung von Lösegeldern. Dies hat sich jedoch mit dem Aufkommen der IABs geändert. Diese Angreifer konzentrieren sich darauf, Zugang zu Netzwerken zu erlangen und dann diesen Zugang an andere Kriminelle zu verkaufen.

Die IAB verfügen oft über begrenzte Fähigkeiten und sind nicht in der Lage, Malware zu entwickeln oder ausgefeilte Ransomware-Programme auszuführen. Sie machen häufig Profit, indem sie Zugang zu vielen Organisationen an andere Cyberkriminelle verkaufen, um ihn in Angriffen zu nutzen. Die Vereinbarung ist auch vorteilhaft für Ransomware-Banden und andere Gruppen fortgeschrittener anhaltender Bedrohungen, die oft durch die Anzahl der Systeme begrenzt waren, die sie hacken konnten. Anstatt spezifische Branchen oder Organisationen zu zielen, sind die Angriffe durch die IAB vergleichsweise unbedacht. Sie nutzen oft bekannte Schwachstellen und suchen nach jedem verwundbaren Asset am Rand einer Organisation, das sie ausnutzen können. Mit der Etablierung der IAB wird erwartet, dass Ransomware-Banden in der Lage sein werden, eine zunehmende Anzahl von Organisationen anzugreifen.



25,059

CVE-Einträge wurden im Jahr 2022 veröffentlicht, was einem Anstieg von etwa 25 % gegenüber 2021 entspricht.

15 Minuten

nach einer CVE-Ankündigung beginnen Bedrohungsakteure laut Forschung mit dem Scannen des Internets.

Die bestehenden Prozesse können nicht Schritt halten

Traditionelle Programme zur Verwaltung von Schwachstellen sind nicht mehr geeignet

Das Prinzip der Schwachstellenverwaltung ist einfach: Organisationen priorisieren Schwachstellen basierend auf ihrer Schwere und dem Risikoniveau, das sie darstellen. Jedoch, wie gezeigt, erfolgen Verletzungen unter Ausnutzung von Schwachstellen weiterhin in hohen Raten. Programme zur Schwachstellenverwaltung kämpfen in der Regel aus drei Gründen:

- **Mangel an Sichtbarkeit** – Damit Programme zur Schwachstellenverwaltung funktionieren, müssen Organisationen ihre Angriffsfläche kennen. Jedoch haben Organisationen laut Forrester durchschnittlich eine um 30% größere Angriffsfläche, als sie dachten.
- **Ineffiziente Entdeckung** – Das Identifizieren von Schwachstellen auf der Angriffsfläche präsentiert zwei Herausforderungen; die erste ist, so viele wie möglich zu identifizieren, denn die übersehenen könnten zu einem Bruch führen. Die zweite ist, die Anzahl der Falschpositiven zu minimieren, die die Teams verlangsamen und sie daran hindern, sich um die echten Risiken zu kümmern.
- **Ungenau Priorisierung** – Viele Organisationen scheitern daran, Schwachstellen richtig zu priorisieren und konzentrieren sich stattdessen darauf, Schwachstellen basierend auf ihrem Alter oder dekontextualisierten Scores wie dem CVSS zu beheben. Dieser Ansatz kann dazu führen, dass kritische Risiken unbehandelt bleiben, was zu Sicherheitsverletzungen führen kann.

56%

der Großunternehmen verwalten täglich mehr als 1.000 Sicherheitswarnungen.

66%

der Sicherheitsteams sagen, dass es schwierig ist, komplexe und sich ständig verändernde Angriffsflächen zu schützen.

68%

aller Cyberangriffe nutzen Schwachstellen aus, für die bereits seit mehr als einem Jahr ein Patch verfügbar war.

Ein moderner Ansatz für ein modernes Problem

Einführung in das Continuous Threat Exposure Management (CTEM)

Das Continuous Threat Exposure Management (CTEM) ist die kontinuierliche Überwachung und Identifizierung von Bedrohungen, Schwachstellen und Risiken in Echtzeit. Es ermöglicht Organisationen, schnell auf Bedrohungen zu reagieren und das Risiko eines erfolgreichen Angriffs zu reduzieren.

> Bis 2026 werden Organisationen, die ihre Sicherheitsinvestitionen auf der Grundlage eines Programms für kontinuierliches Exposure-Management priorisieren, dreimal weniger wahrscheinlich einen Sicherheitsbruch erleiden.
>
> **Gartner**

Die Art und Weise, wie Sie Risiken reduzieren, ist einzigartig für Ihre Organisation, aber CTEM bietet die Architektur, um die Herausforderungen zu bewältigen, denen Sie gegenüberstehen:

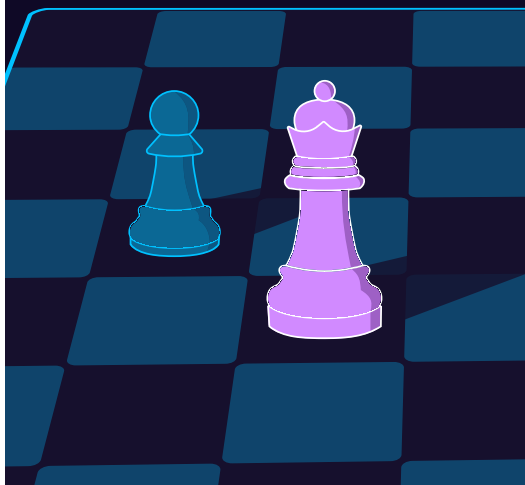
- Minimierung der Anzahl von Sicherheitsvorfällen, mit denen Organisationen derzeit konfrontiert sind.
- Schaffung sicherer Umgebungen in sich ständig verändernden Kontexten.
- Identifizierung von Schwachstellen in Ihrer Sicherheitslage, die ein Angriff ausnutzen könnte.
- Verringerung des Risikos, das durch Technologie entsteht, welche die Arbeit aus der Ferne unterstützt.
- Verlagerung kritischer Geschäftsfunktionen auf Drittanbieterdienste oder -plattformen.

87%

der Führungskräfte priorisieren die digitale Transformation als organisatorische Priorität, laut dem Gartner-Bericht.

85%

der Führungskräfte priorisieren die digitale Transformation als organisatorische Priorität, laut dem Gartner-Bericht.



Das Verständnis des Expositionsmanagements

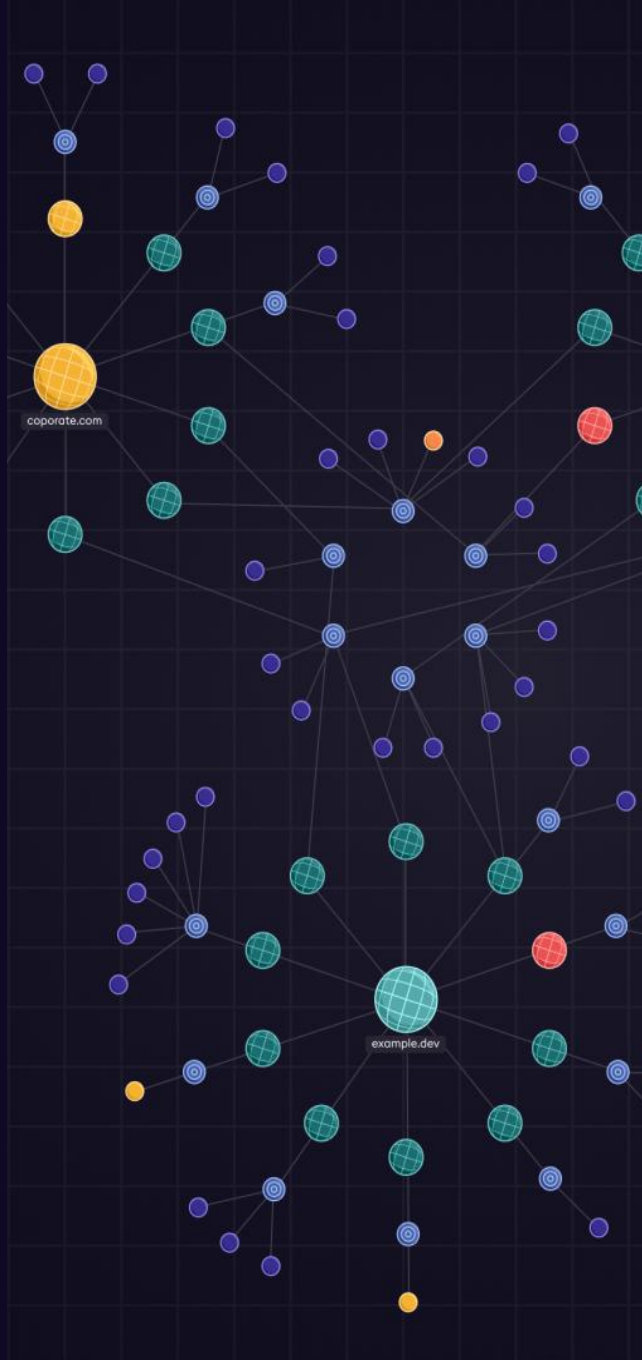
Bietet, was die Schwachstellenverwaltung nicht kann

Programme für das Expositionsmanagement gehen in mehreren Bereichen über die Schwachstellenverwaltung hinaus:

- **Bewertung der Sicherheitslage**, indem die gesamte Angriffsfläche Ihrer Organisation einbezogen wird, nicht nur die bekannten und manuell katalogisierten Assets.
- **Bestimmung der Wahrscheinlichkeit und des Auswirkungsgrads** einer Ausnutzung basierend auf der gesamten Umgebung der Organisation, nicht nur indem das Risiko in isolierten Fällen betrachtet wird.
- **Empfehlung von Abhilfemaßnahmen**, damit die breitere Organisation sie umsetzt, nicht nur die Teams, die für die Behebung von Schwachstellen verantwortlich sind.

Um ein Expositionsmanagementprogramm erfolgreich zu implementieren, sind mehrere Fähigkeiten erforderlich:

- Kontinuierliche Entdeckung nach außen gerichteter Assets.
- Autonome Erkennung ausnutzbarer Risiken.
- Präzise Risikopriorisierung.
- Bestätigung, dass die Risiken behoben wurden.



Hadrians Orchestrierer

Verhinderung von Verletzungen durch Expositionsmanagement

Hadrian bietet eine kontinuierliche Abdeckung des Lebenszyklus des Managements externer Expositionen, um Risiken zu reduzieren, Effizienz zu verbessern und Compliance zu vereinfachen. Im Herzen unserer Plattform steht der Orchestrierer, der 24x7x365 Analysen durchführt, wie ein realer Gegner, indem er dynamisch mehr als 200 "Hacker"-Module verbindet.

1

Assets

Der Orchestrierer entdeckt unbekannte Assets, indem er täglich 1,1 Tb Daten verarbeitet, um jedes Ihrer Organisation gehörende Asset zu entdecken. Um unangenehme Überraschungen zu vermeiden, scannt der Orchestrierer kontinuierlich nach Anzeichen neuer Assets und Veränderungen.

2

Kontext

Die Hadrian-Plattform kontextualisiert Ihre Assets, um zu verstehen, wie ein Gegner einen Angriff durchführen würde. Hadrian identifiziert Informationen über das Betriebssystem, Module, Bibliotheken, Eingabefelder, Authentifizierungsmethoden und vieles mehr in dieser Phase.

3

Risiken

Der Orchestrierer nutzt sein Wissen über Ihre Umgebung, um Schwachstellen zu sondieren, lernt dabei und verfeinert die Techniken, die er verwendet. Hadrian identifiziert zuverlässig zuvor unentdeckte Risiken für Ihre Organisation mit weniger Falschpositiven.

HADRIAN

Hadrian ist ein führender Anbieter von Lösungen für das Management der Externen Angriffsfläche (EASM), Kontinuierliches Automatisiertes Red Teaming (CART) und Continuous Threat Exposure Management (CTEM). Unsere Plattform katalogisiert bekannte und unbekannte Assets, wo immer sie sich befinden, untersucht Schwachstellen, indem sie Exploits ausführt, wie es ein Bedrohungsakteur tun würde, und priorisiert Risiken für eine schnelle Behebung basierend auf Ihrer einzigartigen Umgebung.

Demo buchen | Mehr erfahren

(1) Forrester, Infrastructure Cloud Survey (2022)
(2) Owl Labs, State of Remote Work (2022)
(3) Gartner, Speed Up Your Digital Business Transformation (2019)
(4) ESG, Security Hygiene and Posture Management (2022)
(5) Madiant, Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace (2023)
(6) CVE, Metrics webage (accessed April 2023)
(7) Palo Alto, Incident Response Report (2022)
(8) Sumo Logic, State of SecOps and Automation (2020)
(9) Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019)
(10) Abdalslam, Patch Management Statistics, Trends And Facts (2023)
(11) Cloud Native Computing Foundation, Cloud Native Security Microsurvey (2021)

Vertrauenswürdig von

BIOLANDES | CTC GLOBAL | beyond. | KCK | KINGSWAY CAPITAL | bank prov. | LEROY MERLIN | London Business School