HADRIAN

Offensive Sicherheit. Vereinfacht

Defensive Kontrollen mit automatisierter Offensive Sicherheit validieren

Autonom

Hadrian validiert Risiken in Ihrer gesamten Organisation mit denselben Methoden wie ein Penetrationstester. Das berührungsfreie Design simuliert einen Sicherheitsexperten ohne Konfiguration, Planung und manuellen Eingriff. Ergebnisse werden automatisch auf Genauigkeit und Zuverlässigkeit geprüft.

Kontinuierlich

Hadrian bietet Echtzeit-Einblick in die Bedrohungslage Ihrer Angriffsfläche. Die ereignisbasierte Architektur überwacht Ihre Angriffsfläche 24/7/365 auf Veränderungen, die ein Angreifer ausnutzen könnte. Untersuchungsscans werden ausgelöst, sobald eine mögliche Bedrohung erkannt wird, sodass Sie jederzeit vollständig informiert sind.

Umfassend

Hadrian führt umfangreiche und tiefgehende Tests durch, um Exploits aufzudecken und zu validieren. Der Orchestrator AI wird von unseren internen Hackern geschult und aktualisiert, um Angriffe aus der realen Welt zu simulieren und Bedrohungen zu entdecken, die andere Tools nicht finden können. Die automatisierten Penetrationstests sind vergleichbar mit denen von menschlichen Operatoren.

Haupteinsatzfälle

Automatisiertes Penetrationstesting
Verhindern Sie Datenverletzungen, indem Sie kontinuierlich echte Cyberangriffe simulieren, um Exploits zu entdecken, bevor Cyberkriminelle dies tun.

Kontinuierliche Angriffsflächen-Erkennung
Schnell Angriffsvektoren in dynamischen Umgebungen mit Echtzeit-Überwachung für internetzugängliche assets identifizieren..

Bedrohungsexpositionsmanagement
Effizient Sicherheitsbedrohungen mit End-to-End-Automatisierung des Risikoerkennungs-, Validierungs- und Behebungs-Workflows mindern.

Risikobasiertes Schwachstellenmanagement
Eliminieren Sie die Risiken, die am wichtigsten sind, mit intelligenter Priorisierung, die den Geschäftseinfluss und die Wahrscheinlichkeit der Ausnutzung berücksichtigt.

Gesteuert vom Orchestrator AI

Hacker verstehen Hacker am besten. Unser Orchestrator AI repliziert ein Team von Hackern, das Ihre Organisation rund um die Uhr bewacht, um Risiken zu entdecken und zu validieren.

Schritt 1: Entdeckung

Unser Orchestator AI entdeckt alle Ihre externen Assets mit einem Graph Neural Network dass das Internet analysiert. Machine Learning-Algorithmen, die Text, Bilder, Skripte, DNS-Einträge und zahlreiche andere Merkmale überprüfen, identifizieren Assets.

Schritt 2: Kontextualisierung

Hadrians Plattform kontextualisiert Ihre Assets, um zu verstehen, wie ein Gegner einen Angriff durchführen würde. Hadrian erfasst Informationen zu Betriebssystemen, Modulen, Bibliotheken, Eingabefeldern, Authentifizierungsmethoden und vielem mehr.

Schritt 3: Validierung

Orchestrator AI nutzt Wissen über Ihre Angriffsfläche, um OWASP Top Ten-Risiken, Schwachstellen und Dienstfehler zu prüfen, indem Scans kombiniert werden, um komplexe multidimensionale Angriffe zu simulieren.

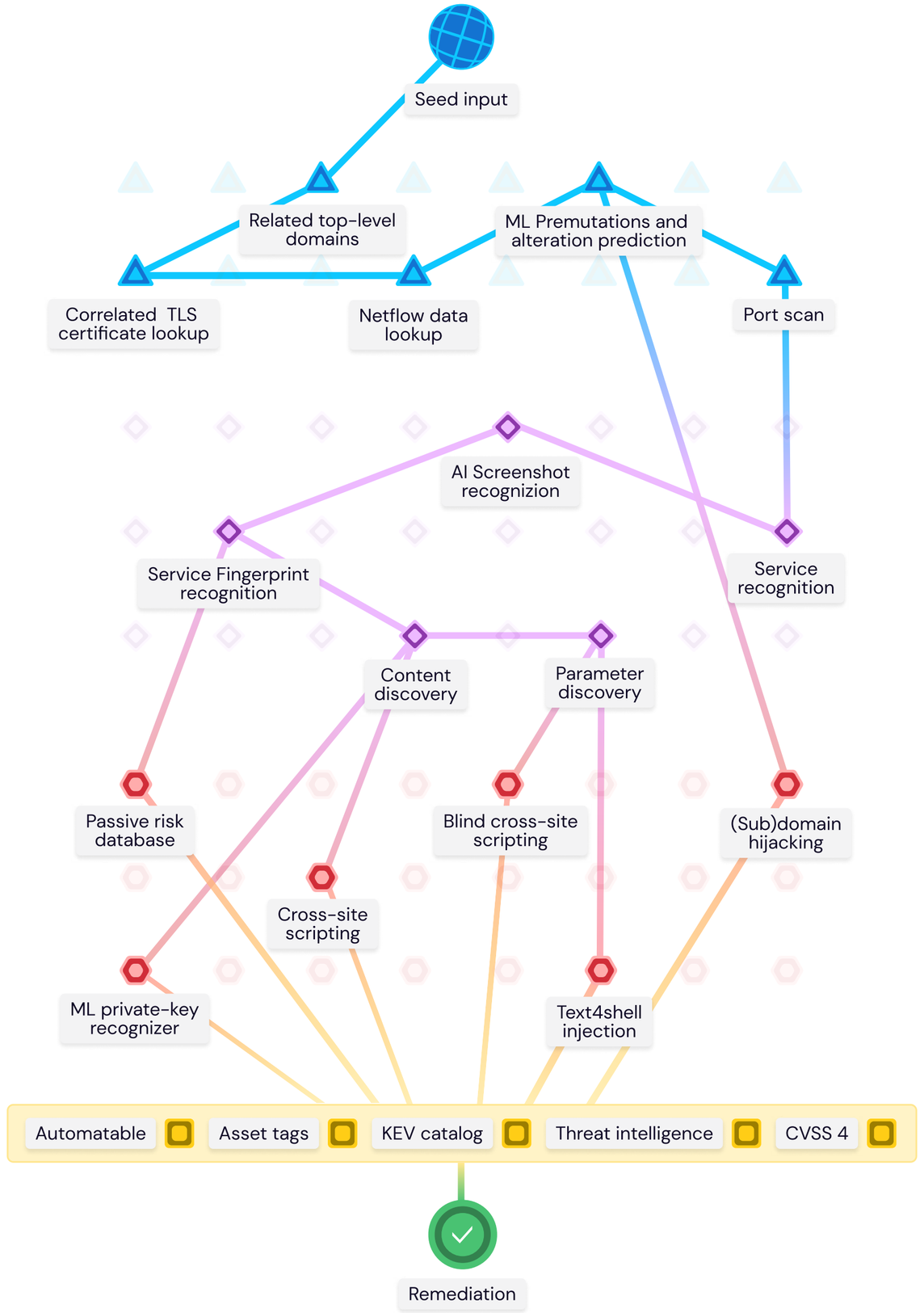
Schritt 4: Priorisierung

Hadrian priorisiert validierte Risiken basierend auf technischen Faktoren, der Wahrscheinlichkeit einer Ausnutzung und potenziellen Geschäftsauswirkungen. Die proprietären Scoring-Algorithmen lernen aus Benutzerfeedback, um genauer zu werden.

Schritt 5: Behebung

Orchestrator AI vereinfacht die Behebung, indem es relevanten Geschäftseinheiten umsetzbare, schrittweise Anweisungen zur Lösung von ausnutzbaren Risiken bereitstellt. Validierung durchgeführt, um zu bestätigen, dass die Behebung erfolgreich war.

Orchestrator AI's event-driven architecture



Die Hacker-Perspektive

Defensive Sicherheit sollte durch offensive Sicherheit validiert werden. Hadrian bietet die Hacker-Perspektive und zeigt die Ziele und Methoden auf, die bei einem realen Datenverstoß verwendet werden könnten. Hadrians kontinuierliche und umfassende Tests entdecken und validieren Risiken vollständig autonom.

Hadrians Plattform kombiniert die Entdeckung der Angriffsfläche, automatisiertes Penetrationstesten und Technologien zum Management von Risikenbedrohungen in einer cloud-basierten und agentenlosen Plattform. Die Spitzentechnologie wird ständig von Hadrians internem Hacker-Team aktualisiert und verbessert.

+200	+1,2m	+3.5 TB
geschützte Unternehmen	gesicherte Assets	täglich verarbeitete Daten

Vertraut von

ABN·AMRO | SHV ENERGY | macmillan education

WeatherTech | LEROY MERLIN | LOTTOMATICA

RITUALS... | BIOLANDES | nedap

> „Was an dem, was Hadrian macht, spannend ist, ist, dass sie ein scheinbar unmögliches Puzzle gelöst haben: das Auffinden von Schwachstellen in einem komplexen Netzwerk mit menschenähnlichen Details, im großen Maßstab, von außen und kontinuierlich. Was normalerweise ein engagiertes Team von Sicherheitsingenieuren ein paar Wochen für ein System benötigt, können sie in Minuten für Tausende von Systemen tun."
>
> **Tiago Teles, Sicherheitsleiter bei ABN AMRO**

Vereinfachen Sie offensive Sicherheit und bewältigen Sie validierte Risiken mit weniger Aufwand.

Erfahren Sie mehr auf **hadrian.io**

Kontaktieren Sie uns unter **info@hadrian.io**