HADRIAN

Die Hacker-Perspektive

Agentisches Hacking identifiziert, validiert und priorisiert Schwachstellen, bevor Angreifer zuschlagen. Mit Hadrian kann agentische KI proaktiv die OWASP Top Ten-Probleme, Zero-Day- und bekannte Schwachstellen sowie Fehlkonfigurationen in Ihrer gesamten externen Angriffsfläche finden und mindern.

Kommen Sie Ihren Angreifern zuvor und verhindern Sie Sicherheitslücken, bevor diese einen Angriff starten können. Hadrian hilft Ihnen, von einem reaktiven zu einem proaktiven Cybersecurity-Ansatz überzugehen, indem es die Verwaltung der Angriffsoberfläche, die Überprüfung der Gefährdung durch Angreifer und die Verwaltung der Bedrohungslage automatisiert.

Hadrian überwacht kontinuierlich Ihre gesamte digitale Infrastruktur – On-Premise und in der Cloud – und liefert dabei in Echtzeit verwertbare Sicherheitseinblicke. Durch diese Automatisierung können sich Ihre Sicherheitsteams auf die wichtigsten Risiken konzentrieren, um Sicherheitsvorfälle zu verhindern und Ihre Sicherheitslage über die gesamte Angriffsfläche hinweg zu verbessern.

Was Hadrian anders macht

- **Immer aktiv**

  Im Gegensatz zu herkömmlichen Tests, die in regelmäßigen Abständen durchgeführt werden, läuft Hadrian rund um die Uhr und gewährleistet so Echtzeitsichtbarkeit und Schutz vor neuen Bedrohungen.

- **Hohe Genauigkeit**

  Hadrian reduziert Fehlalarme durch KI-gestützte, gegnerische Tests zur Validierung von Schwachstellen. So reagieren Ihre Sicherheitsteams nur auf echte, ausnutzbare Risiken.

- **Sofortiges Deployment**

  Hadrian erfordert keine aufwendige Einrichtung oder Wartung und liefert sofortige Einblicke in Ihre Angriffsfläche – ohne den laufenden Betrieb zu beeinträchtigen.

Wichtigste Vorteile

Assets entdecken

Erhalten Sie in Echtzeit Einblick in Ihre digitalen Assets – durch automatische Erkennung und Kontextualisierung. Die Asset-Inventarisierung von Hadrian spart Kunden im Durchschnitt über 10 Stunden pro Woche.

Exponierungen aufdecken

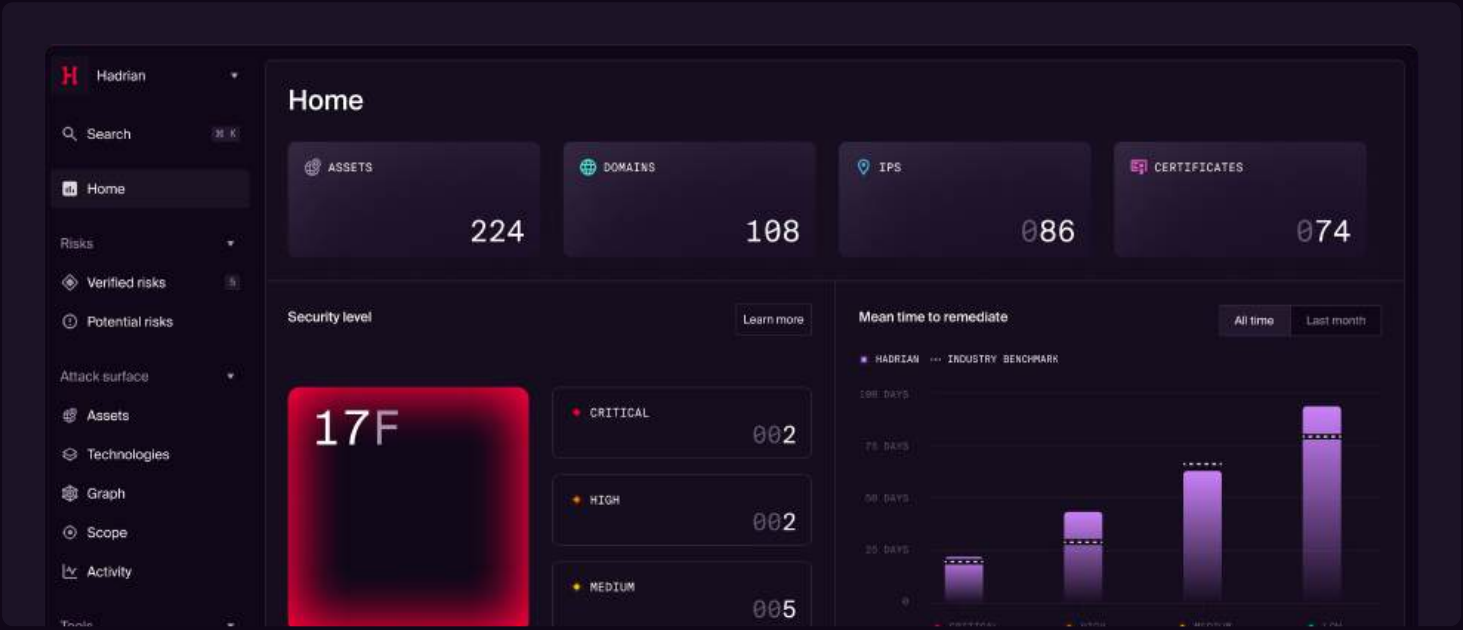
Erhalten Sie mit detaillierten Bewertungen ein zehnfach besseres Verständnis kritischer Risiken. Hadrians modulare Architektur zur Bedrohungsbewertung bildet reale Hackertechniken und -verhaltensweisen praxisnah ab.

Probleme beheben

Reduzieren Sie die MTTR um 80 % mit optimierten Workflows und flexiblen Integrationen. Hadrian bietet Schritt-für-Schritt-Anweisungen zur Behebung von Problemen und eine Reihe von Tools für die Zusammenarbeit, um die Lösung zu beschleunigen.

HADRIAN

Hadrians Offensive Sicherheitsplattform



Outside-In-Perspektive

Hadrian analysiert kontinuierlich Ihre externe Angriffsfläche und identifiziert Schwachstellen – genau wie es ein echter Angreifer tun würde.

KI-gesteuerte Tests

Automatisierte, KI-gestützte Tests simulieren reale Angriffstechniken, um Schwachstellen präzise aufzudecken.

Ereignisgesteuerte Architektur

Hadrian reagiert in Echtzeit auf Veränderungen in Ihrer Umgebung und stellt sicher, dass Bedrohungen unmittelbar erkannt werden.

Kontextabhängige Prioritätensetzung

Durch intelligente Risikobewertung konzentrieren sich Ihre Sicherheitsteams auf die kritischsten, tatsächlich ausnutzbaren Schwachstellen.

Zero-Touch-Deployment

Hadrian kommt ohne Agenteninstallation aus und ermöglicht sofortige Einblicke in Ihre Angriffsfläche – ohne Eingriffe in bestehende Systeme.

Nahtlose Integration

Einfache Anbindung an bestehende Sicherheits-Workflows erhöht Ihren Schutz – ohne zusätzliche Komplexität.

Klassenbester

Die offensive Sicherheit von Hadrian zeigt, wie reale Angriffe Anwendungen und Infrastrukturen gefährden könnten. Unsere autonome Plattform führt kontinuierlich Tests durch, um Ihre mit dem Internet verbundenen Ressourcen umfassend zu bewerten. Die cloudbasierte, agentenlose Technologie wird von Hadrians ethischem Hacker-Team ständig aktualisiert und weiterentwickelt.

FROST & SULLIVAN BEST PRACTICES AWARDS

Gartner Peer Insights 4.9/5 ★

GIGAOM RADAR REPORT LEADER 2025

AICPA SOC

ISO 27001