

Pentests agentic autonomes sur l'ensemble de la surface d'attaque externe



Atténuez les menaces de manière proactive en combinant l'instinct du hacker et l'évolutivité de l'IA agentielle. Hadrian révèle les vulnérabilités exploitables en évaluant en permanence les menaces avec la précision d'une équipe de testeurs d'intrusion de classe mondiale. Adoptez une sécurité offensive et remédiez à vos expositions critiques avec moins d'efforts.

- DÉTECTION CONTINUE
- INFORMATIONS DE NIVEAU PENTEST, 24H/24, 7J/7
- VALIDATION DE L'EXPOSITION ANTAGONISTE AUTONOME
- ZERO INSTALLATION

■ DÉCOUVREZ TOUT

10x

visibilité des expositions critiques

Bénéficiez d'une visibilité en temps réel sur chaque ressource et exposition de votre surface d'attaque numérique. L'analyse 24h/24, 7j/7 et 365j/an d'Hadrian vous permet d'être pleinement informé à tout moment, minimisant ainsi la fenêtre de vulnérabilité.

■ AUTOMATISATION DE LA VALIDATION

10h

gagnées par semaine (en moyenne)

Concentrez-vous sur les risques exploitables et éliminez les faux positifs grâce à des tests de pénétration approfondis. Les évaluations entièrement automatisées d'Hadrian sont discrètes et enrichies d'informations sur les menaces.

■ RÉOLUTION PLUS RAPIDE

80%

réduction du MTTR

Accélérez le temps de réponse et améliorez considérablement votre posture de sécurité. Hadrian déclenche et orchestre des workflows afin de rationaliser la remédiation et d'empêcher les acteurs malveillants de mener leurs attaques.

La sécurité offensive devient proactive

Les cadres traditionnels d'orchestration de la sécurité reposent encore sur des manuels que les humains doivent maintenir à jour. Les pirates ne se contentent pas de suivre des manuels. Ils improvisent. Hadrian remplace l'orchestration lente et fastidieuse par des agents IA pirates autonomes qui pensent et agissent comme des adversaires, sondant votre environnement 24 heures sur 24, 7 jours sur 7.

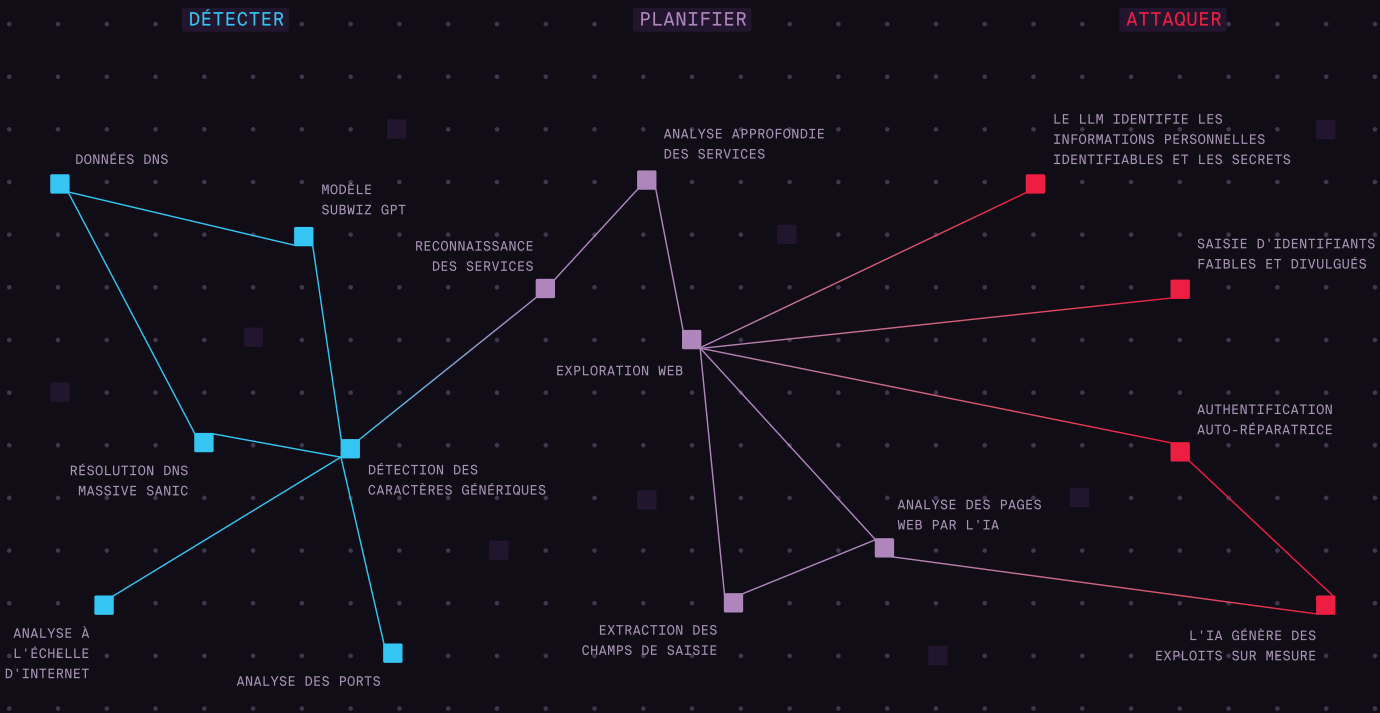
- Une seule couche de données collecte et corrèle tous les signaux provenant de votre surface d'attaque externe.
- Les agents IA du hacker décident de manière autonome quand les actifs nécessitent une enquête plus approfondie et tentent d'exploiter les vulnérabilités.
- Le moteur Adversary forme les agents à s'enchaîner, à imiter les attaquants du monde réel et à exécuter des modèles d'attaque complexes.

Les tests Agentic remplacent les tests d'intrusion

Oubliez les tests de pénétration annuels qui sont déjà obsolètes au moment où le rapport arrive. Hadrian simule en continu le comportement des adversaires, validant chaque modification apportée à votre infrastructure au fur et à mesure, pour un coût bien inférieur à celui des tests manuels. Résultat : réduction du temps d'exposition, efficacité opérationnelle accrue et améliorations mesurables en matière de sécurité.

- Visibilité en temps réel des nouvelles expositions dès qu'elles deviennent exploitables, ce qui évite d'attendre des semaines ou des mois pour obtenir un rapport.
- Une portée infinie signifie qu'Hadrian découvre automatiquement de nouveaux actifs et expositions sans avoir besoin de cibles prédéfinies. Fini les angles morts.
- La hiérarchisation basée sur le contexte utilise l'IA pour attribuer des scores de gravité en fonction du contexte commercial et de l'impact afin de garantir que votre équipe se concentre sur les risques les plus importants.

Plateforme de tests d'intrusion proactive d'Hadrian



Découvrez le point de vue des hackers

En adoptant le point de vue d'un pirate informatique, la plateforme Hadrian se concentre sur les voies d'attaque et les vulnérabilités qui ont une incidence réelle, et non sur des problèmes théoriques ou à faible risque. Cela réduit le bruit et les faux positifs pour les équipes de sécurité et leur permet de remédier aux risques les plus importants.

Détecter

À l'instar d'un véritable attaquant, les agents du hacker recherchent sur Internet vos actifs exposés et vos points d'entrée ouverts, améliorant ainsi de 10 fois votre visibilité sur les expositions critiques.

Planifier

Les agents du hacker établissent des liens entre les actifs afin de devancer les hackers qui planifient leur prochaine attaque.

Attaquer

Enfin, les agents travaillent ensemble pour vérifier si une voie d'attaque est réellement exploitable ou seulement théorique, fournissant ainsi des informations exploitables et étayées par des preuves auxquelles vous pouvez vous fier.

HADRIAN

Hadrian is an agentic pentesting platform that continuously uncovers and validates exploitable exposures across your entire external attack surface like a real-world adversary. By combining the instincts of a hacker with autonomous AI agents, Hadrian delivers 24/7 adversarial testing and actionable insights that help security teams reduce exposure time and focus on what truly matters.

APPROUVÉ PAR LES LEADERS DU MARCHÉ

