HADRIAN

Sécurité Offensive. Simplifiée

Validez les contrôles défensifs avec une sécurité offensive automatisée

Autonome

Hadrian valide les risques dans l'ensemble de votre organisation en utilisant les mêmes techniques qu'un “pentester”. La conception sans contact simule un expert en sécurité sans configuration, sans programmation et sans intervention manuelle nécessaire. Les résultats sont automatiquement triés en fonction de leur exactitude et de leur fiabilité.

Continu

Hadrian offre une visibilité en temps réel de l'exposition aux menaces dans votre environnement. L'architecture basée sur les événements surveille votre surface d'attaque 24 heures sur 24, 7 jours sur 7 et 365 jours par an pour détecter les changements qu'un acteur menaçant pourrait exploiter. Les analyses d'investigation sont déclenchées dès qu'une menace potentielle est détectée, ce qui vous permet de rester informé en permanence.

Complet

Hadrian effectue des tests étendus et approfondis pour découvrir et valider les exploits. L'IA de l'orchestrateur de la plateforme est formée et mise à jour par nos hackers internes afin d'émuler des attaques réelles et de découvrir des menaces que d'autres outils ne peuvent pas détecter. Les capacités de tests de pénétration automatisés rivalisent avec celles des opérateurs humains.

Principaux cas d'utilisation

Test de pénétration automatisé
Prévenez les violations de données en simulant continuellement des cyberattaques réelles afin de découvrir des failles avant les cybercriminels

Découverte continue de la surface d'attaque
Identifiez rapidement les vecteurs d'attaque dans des environnements dynamiques grâce à la surveillance en temps réel des actifs en contact avec Internet

Gestion de l'exposition aux risques
Atténuez efficacement les menaces de sécurité grâce à une automatisation complète des processus de détection des risques, de validation et de remédiation

Gestion des vulnérabilités basée sur le risque
Éliminez les risques les plus importants avec une priorisation intelligente qui prend en compte l'impact commercial et la probabilité d'exploitation

Propulsé par Orchestrator IA

Les hackers sont ceux qui connaissent le mieux les hackers. Orchestrator IA reproduit une équipe de hackers évaluant votre organisation en continu pour découvrir et valider vos risques.

Étape 1: Découverte

L'Orchestrator IA découvre tous vos actifs accessibles depuis l'extérieur en utilisant son graphe de réseau neuronal d'internet. Des algorithmes d'apprentissage automatique qui examinent le texte, les images, les scripts, les enregistrements DNS et de nombreuses autres caractéristiques identifient les actifs.

Étape 2: Contextualisation

La plateforme d'Hadrian contextualise vos actifs pour comprendre comment un adversaire mènerait une attaque. Hadrian identifie les informations OS, les modules, les bibliothèques, les champs de saisie, les méthodes d'authentification et bien plus encore.

Étape 3: Validation

Orchestrator AI utilise sa connaissance de votre environnement pour tester les risques exploitables du Top Dix OWASP, les vulnérabilités connues et celles de jour zéro, et les services exposés et mal configurés. Les scans sont reliés entre eux pour simuler des attaques multidimensionnelles complexes.

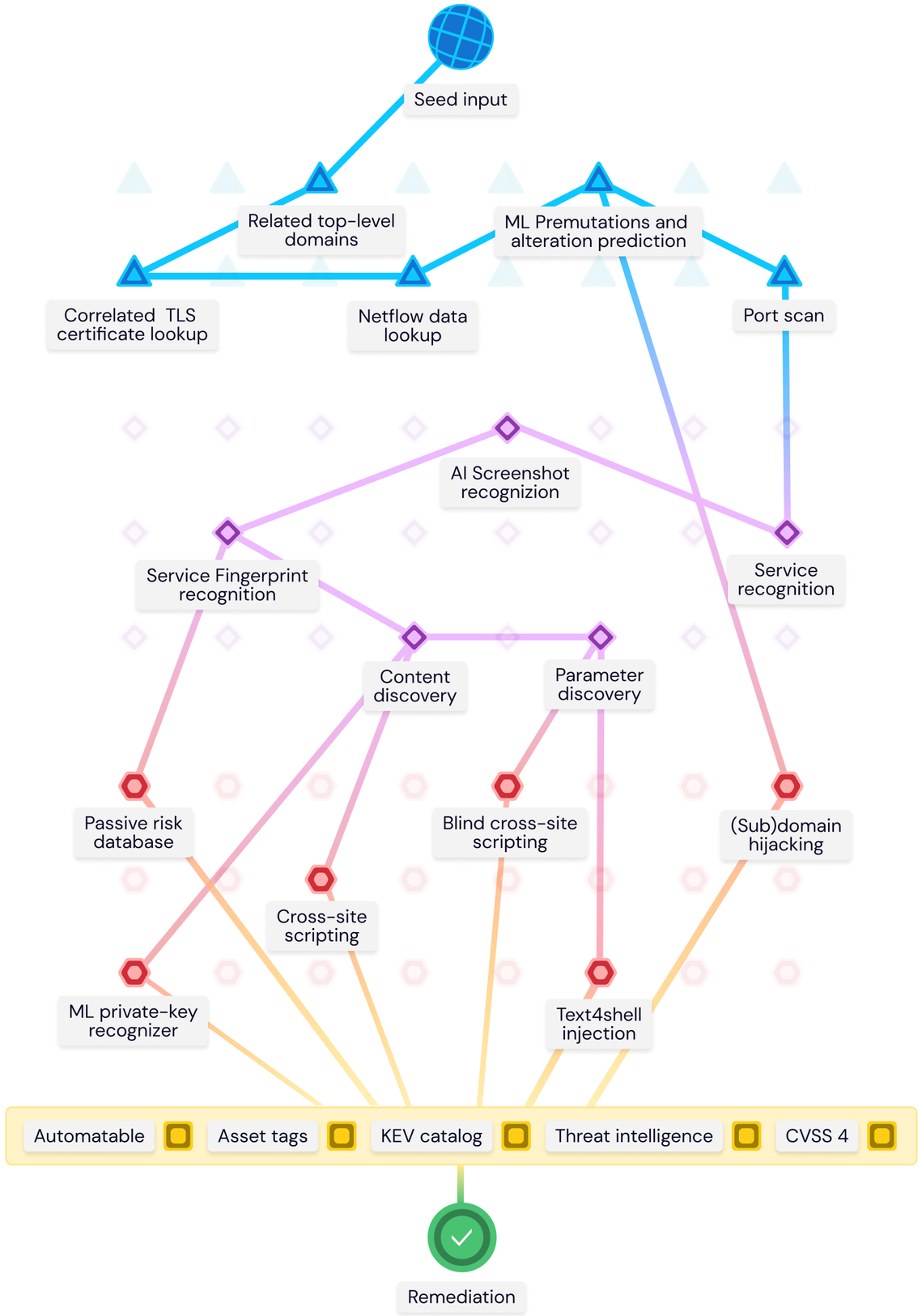
Étape 4: Priorisation

Hadrian priorise les risques validés en fonction de facteurs techniques, de la probabilité d'exploitation et de l'impact commercial potentiel. Les algorithmes de notation exclusifs apprennent des commentaires des utilisateurs pour devenir plus précis.

Étape 5: Remédiation

Orchestrator IA simplifie la remédiation en fournissant aux unités commerciales pertinentes des instructions de résolution étape par étape pour les risques exploitables. Des tests de suivi sont effectués pour confirmer que la remédiation a été réussie.

Orchestrator IA's event-driven architecture



La perspective du hacker

La sécurité défensive devrait être validée par la sécurité offensive. Hadrian fournit la perspective du hacker, révélant les cibles et les méthodes qui pourraient être utilisées dans une véritable violation de données. Les tests continus et complets de Hadrian découvrent et valident les risques de manière totalement autonome.

La plateforme d'Hadrian combine la découverte de la surface d'attaque, les tests d'intrusion automatisés et les technologies de gestion de l'exposition aux menaces dans une plateforme sans agent et basée sur le cloud. La technologie de pointe est constamment mise à jour et améliorée par l'équipe de hackers internes d'Hadrian.

+200	+1,2m	+3,5 To
entreprises protégées	million d'actifs sécurisés	de données traitées quotidiennement

Approuvé par

ABN·AMRO | SHV ENERGY | macmillan education

WeatherTech | LEROY MERLIN | LOTTOMATICA

RITUALS... | BIOLANDES | nedap

> ‘Ce qui est génial avec ce que fait Hadrian, c'est qu'ils ont résolu un puzzle apparemment impossible : trouver des faiblesses dans un réseau complexe avec un niveau de détail humain, à grande échelle, de l'extérieur et de manière continue. Ce qui prend normalement à une équipe dédiée d'ingénieurs en sécurité quelques semaines à comprendre pour un système, ils peuvent le faire en quelques minutes pour des milliers de systèmes.’
>
> **Tiago Teles, responsable de la sécurité chez ABN AMRO**

Simplifiez votre sécurité offensive et remédiez aux risques validés avec moins d'effort.