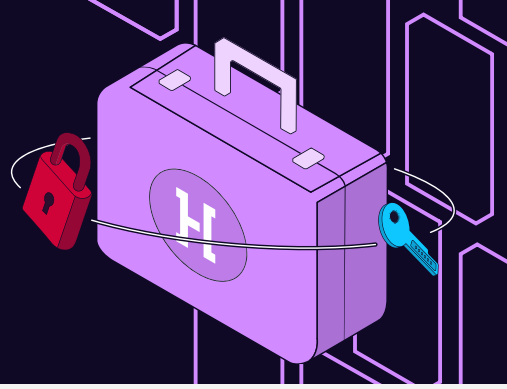
HADRIAN

# Gestion des Expositions pour le Secteur de la Santé



Face à une  menace croissante, les établissements de santé en France font face à une augmentation des cyberattaques, les classant désormais au  3ème rang des secteurs les plus touchés en France. Les infrastructures obsolètes et l'explosion des données de santé exacerbent les risques, nécessitant une action urgente en cybersécurité.

## Principaux Défis

### Le Cloud en Santé

L'adoption du cloud en santé est vitale mais confrontée à des obstacles, comme le manque de compréhension et les préoccupations sur la sécurité. La collaboration entre prestataires, organismes de santé et décideurs politiques est essentielle pour assurer une transition sécurisée vers le cloud.

### Les Nouveaux Services Numériques

Ajouter de nouveaux services numériques sécurisés répond à la demande croissante des clients tout en renforçant la confiance dans notre engagement envers leur sécurité en ligne.

### RGPD, NIS2 et Protection des Données des Patients

La conformité à la RGPD et à la directive NIS2 est essentielle pour garantir la protection des données des patients et éviter de lourdes amendes.

### La Vulnérabilité aux Rançongiciels

Les établissements de santé, de par leur interconnexion croissante et la valeur des données médicales, sont particulièrement visés par les attaques Ransomware.

### IoT et Santé

La sécurité des données et des dispositifs est primordiale, mais aussi la précision des données et le coût de mise en œuvre et de maintenance des appareils. Les organisations doivent s'adapter à ces défis pour tirer parti des avantages de l'IoT en santé.

## Exigences de la Solution

### Inventaire complet des actifs

Détection de tous les actifs exposés appartenant à votre organisation.

### Découverte en temps réel

Suivi des changements de la surface d'attaque dès qu'ils se produisent.

### Scans basés sur les événements

Déclenchement d'évaluations d'exploitation pour identifier de nouveaux risques suite aux modifications des actifs.

### Validation des risques

Suppression des faux positifs en vérifiant que les risques sont exploitables.

### Enrichissement du contexte

Priorisation des risques avec des informations sur l'actif, la fonction et la connexion à d'autres actifs.

### Intelligence menaçante native

Amélioration de la priorisation avec des informations sur la probabilité d'exploitation.

### Fonctionnalités de reporting

Évaluation rapide et rapport sur la posture de sécurité de l'organisation et des risques spécifiques.

### Inventaire détaillé des actifs

Pour éclairer l'IT fantôme et réduire les attaques sur les bords.

## La Solution de Hadrian

La plateforme de sécurité offensive pilotée par l'IA de Hadrian est la pierre angulaire de la gestion automatisée des expositions aux menaces. Notre approche unifiée cartographie la surface d'attaque, identifie les risques exploitables, calcule les priorités en utilisant du renseignement sur les menaces, et déclenche des mesures correctives.

### Découverte continue de la surface d'attaque

Obtenez une couverture continue de votre surface d'attaque externe en détectant en temps réel les changements de configuration et les nouveaux actifs exposés à Internet. L'architecture basée sur des événements de Hadrian déclenche automatiquement des tests pour valider rapidement les risques dès leur découverte.

La nature toujours active de la plateforme vous tient informé 24h/24, 7j/7, 365 jours par an et garantit l'absence de lacunes en termes de visibilité. La plateforme recherche automatiquement de nouveaux actifs et effectue des tests de régression pour vérifier que les risques ont été résolus avec succès.

### Tests de pénétration automatisés

Hadrian valide les risques exposés à Internet. L'Orchestrator AI est conçu et formé par des hackers white hat de classe mondiale pour utiliser les mêmes techniques qu'un testeur de pénétration humain. La plateforme recherche constamment les vulnérabilités connues et zero-day sans nécessiter de configuration, de planification ou d'intervention manuelle.

L'Orchestrator AI valide la possibilité d'exploitation des menaces, catégorisant les résultats en vrais positifs et expositions potentielles. La plateforme utilise une intelligence des menaces native et le contexte des actifs pour prioriser les risques les plus élevés.

### Remédiation des expositions aux menaces

Résolvez plus rapidement et avec moins d'efforts et de coûts les risques critiques avec les capacités de gestion des expositions de Hadrian. Hadrian permet aux équipes de sécurité de se concentrer sur les risques les plus importants, d'agir immédiatement et de réduire de manière mesurable le MTTR.

Hadrian identifie de manière autonome et continue les expositions dans les surfaces d'attaque externes, produisant des résultats faciles à comprendre et contenant des instructions de reproduction et de remédiation. La plateforme complète facilement les flux de travail existants avec des intégrations dans plus de 100 systèmes SIEM, SOAR et ITSM.

> La plateforme de Hadrian identifie les vulnérabilités de manière plus approfondie que d'autres outils entièrement automatisés. Les connaissances fournies par Hadrian nous ont aidés à renforcer la sécurité de notre système. D'excellents aperçus.
>
> CISO - Leroy Merlin

## À Propos de Hadrian

Hadrian offre la perspective des hackers, révélant les cibles et les méthodes qui pourraient être utilisées dans une violation de données réelle. Notre plateforme basée sur le cloud et sans agent effectue des tests continus et complets pour découvrir et valider les risques de manière entièrement autonome. La technologie de pointe est constamment mise à jour et améliorée par l'équipe interne de hackers de Hadrian.

En savoir plus sur hadrian.io/demo

HADRIAN