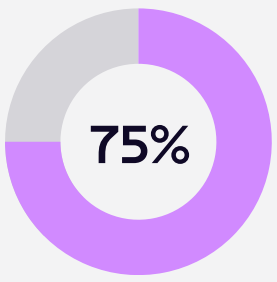
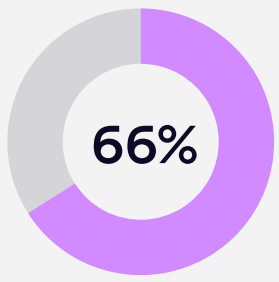
HADRIAN

Le guide du ROI pour la Sécurité Offensive

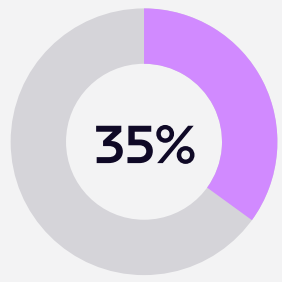
La sécurité offensive complète et valide les investissements existants en cybersécurité en identifiant les lacunes dans les contrôles existants. Les analyses montrent que les responsables de la sécurité investissent de plus en plus dans la sécurité offensive pour identifier et remédier proactivement.



Des risques inconnus amènent **75,2%** des organisations à augmenter leurs pratiques de sécurité offensive[1]



L'accès à distance et les applications exposées sur Internet représentent 39% et 27% des vecteurs d'accès initiaux dans la 1ère moitié de 2023[2]



Suite à une violation, **35%** des organisations investissent dans la sécurité offensive, le 4e investissement le plus courant[3]

Les méthodes traditionnelles de sécurité offensive, telles que les tests de pénétration manuels, le balayage des vulnérabilités et la gestion de la surface d'attaque, peuvent permettre aux risques de passer inaperçus et non résolus. La figure 1 indique les principales préoccupations des professionnels de la sécurité interrogés concernant leur exposition aux menaces externes.

Figure 1 - Principales préoccupations concernant l'exposition aux menaces

Principaux défis auxquels font face les méthodes traditionnelles de sécurité offensive:

Laisse des angles morts

Les outils hérités, tels que l'ASM ou les scanners de vulnérabilités, ne testent qu'une fraction des risques. Les tests humains ne peuvent pas s'étendre pour couvrir l'ampleur des surfaces d'attaque modernes.

Résultats inutilisables

L'efficacité de la remédiation est diminuée par des outils et des rapports contenant des risques non validés et des faux positifs. La priorisation sans contexte entraîne une résolution lente.

Intensif en ressources

Les tests et la configuration d'outils exigent des processus manuels, tout comme la compréhension et l'identification de la remédiation optimale.

Hadrian Security fournit une sécurité offensive de premier ordre afin que les organisations puissent atténuer proactivement les menaces et minimiser les risques. La plateforme continue et autonome offre une couverture complète, faisant de Hadrian une solution pérenne qui peut être déployée pour un large éventail de cas d'utilisation.

Avantages Quantifiables

Défi	Solution
Équipes de sécurité débordées Les équipes de cybersécurité font face à un barrage d'alertes, détournant les ressources et l'attention des tâches de sécurité stratégiques. L'investigation des alertes de sécurité est gourmande en ressources, avec des équipes consacrant en moyenne plus de 25 minutes par alerte. Les outils tiers, tels que les services de notation de sécurité et la gestion de la surface d'attaque, ont exacerbé cette situation en classifiant mal la gravité des vulnérabilités. Cela a sollicité les ressources et entravé la concentration sur les efforts de sécurité cruciaux.	**Priorisation basée sur l'intelligence** Les algorithmes propriétaires de notation des risques de Hadrian permettent aux équipes de sécurité de se concentrer sur les risques les plus importants. Le Centre des Opérations de Sécurité (SOC) peut se concentrer sur les incidents importants, les processus de gestion des vulnérabilités peuvent mieux prioriser les patchs, et les équipes DevSecOps peuvent se concentrer sur les problèmes critiques. La priorisation est effectuée par l'Orchestrateur IA de Hadrian qui prend en compte une série de facteurs incluant la probabilité d'exploitation et l'impact potentiel sur l'entreprise. Les algorithmes de notation propriétaires apprennent des retours des utilisateurs pour devenir plus précis.
Tests tiers coûteux Les tests de pénétration tiers sont coûteux et souvent réalisés sur une base annuelle. La nature périodique des tests signifie que les organisations manquent de visibilité entre les évaluations. De plus, ces tests ont une portée limitée, ce qui signifie que seul un sous-ensemble d'actifs exposés est évalué. Le tarif quotidien typique pour un test de pénétration manuel peut varier de 1000 à 3000 dollars par jour.	**Tests de pénétration automatisés** Les tests de pénétration automatisés de Hadrian émulent le comportement des attaquants réels pour une fraction du coût. Les rapports lisibles par l'homme permettent une remédiation immédiate et des scans de suivi automatiques vérifient si la résolution a été réussie. La plateforme de Hadrian effectue des évaluations de menaces en continu, il n'est pas nécessaire d'attendre le prochain test manuel. Les tests de pénétration automatisés examinent les failles de sécurité 24 heures sur 24, toute l'année.
Licences de sécurité héritées Les outils de sécurité inefficaces ou isolés résultent en des aperçus limités. De plus, les solutions ponctuelles telles que les scanners de vulnérabilités ou les services de notation de sécurité servent souvent des cas d'utilisation très limités. De nombreuses organisations rencontrent des défis pour comprendre l'efficacité de leurs outils de sécurité existants et identifier les domaines à affiner.	**Solution IA de nouvelle génération** Les capacités de sécurité offensive complètes de Hadrian permettent de remplacer totalement ou partiellement les outils existants, économisant des dizaines de milliers par an. Hadrian peut également identifier les infrastructures et les appareils périphériques qui peuvent être décommissionnés, réduisant ainsi davantage les coûts. Le reporting intégré de la plateforme permet à l'organisation de mesurer quantitativement les améliorations de la posture de sécurité réalisées au fil du temps.

Avantages non quantifiables

Défi	Solution
Processus de sécurité lents Les composants essentiels de la gestion des expositions, y compris le processus de planification et de réalisation des tests, la validation des résultats et la recherche de remédiation. Les équipes de sécurité suivent ce processus pour comprendre les chemins d'attaque et fournir des conseils aux équipes de remédiation. Cependant, lorsqu'ils sont effectués manuellement, ces processus prennent énormément de temps. Cela signifie que les ressources de sécurité sont étirées et ne peuvent pas enquêter efficacement sur les problèmes.	**Atténuation continue des risques** Hadrian automatise complètement les processus de découverte, de validation, de priorisation et de remédiation. La plateforme vérifie en continu la posture de sécurité de l'organisation et permet aux équipes de sécurité de s'attaquer proactivement aux vulnérabilités exploitables. L'Orchestrateur IA simplifie la remédiation en fournissant aux unités commerciales des instructions claires pour la résolution des risques exploitables. De plus, la plateforme effectue automatiquement des tests de régression pour confirmer l'efficacité de la remédiation.
Évaluations lors des fusions et acquisitions Lors des fusions et acquisitions (M&A), comprendre et gérer la surface d'attaque des entités nouvellement intégrées est souvent un défi, résultant en des actifs et des risques inconnus associés aux départements IT des filiales acquises qui n'étaient pas entièrement intégrés avec le département IT de l'organisation mère. Sans aperçu de la posture de sécurité, les organisations ne peuvent pas prendre de mesures pour atténuer leur exposition aux risques. Certaines organisations font appel à des tiers pour aider, ce qui peut coûter 250 000 par acquisition.	**Aperçus automatisés des risques** Hadrian élimine le besoin de projets spéciaux pour obtenir un inventaire complet de toutes les filiales et de la surface d'attaque et des risques exposés des partenaires commerciaux. Hadrian identifie efficacement les actifs inconnus, offrant aux organisations une visibilité complète et réduisant la charge de travail pour les équipes internes. Les évaluations de risque en temps réel offrent yne vues sur l'empreinte de l'entreprise. L'Orchestrateur IA découvre et teste tous les actifs externes via son réseau neuronal pour identifier les risques.
Dépenses de conformité Réaliser des tests de pénétration est un composant commun des normes de conformité incluant ISO 27001, SOC2, NIS2, DORA, HIPAA et PCI-DSS. Pour les organisations devant se conformer à la réglementation, la réalisation de ces évaluations peut être un coût supplémentaire. De plus, les organisations peuvent passer des semaines à compiler des rapports pour démontrer leur conformité. Lorsque cela est effectué trimestriellement, cela devient plus efficace.	**Rapports à la demande** Hadrian aide les organisations à répondre aux exigences de tests de pénétration, de gestion des vulnérabilités et des risques. Hadrian effectue en continu des évaluations réduisant les tests supplémentaires qui doivent être coordonnés. Le tableau de bord permet aux équipes de sécurité de surveiller et de démontrer l'efficacité de leurs processus. Les rapports peuvent être générés à la demande et facilement partagés avec les parties prenantes internes et externes.

Inventaire manuel des actifs

Les organisations dépendent de processus manuels chronophages, impliquant des feuilles de calcul et des scripts manuels, pour inventorier leurs actifs numériques. Les équipes passent du temps à maintenir les scripts et à dédoublonner les résultats qu'ils produisent.

Il est estimé que 10 minutes de temps d'ingénieur par actif sont nécessaires pour inventorier manuellement les actifs. Cette charge de travail et la précision limitée des données entravent la surveillance de la surface d'attaque en raison du manque d'automatisation et des mises à jour peu fréquentes.

Découverte automatisée continue

La plateforme Hadrian trouve et catalogue les actifs en continu pour construire un inventaire précis et toujours à jour. Les résultats peuvent être facilement examinés dans plusieurs formats basés sur des tableaux et graphiques, ou exportés pour une analyse externe.

Les algorithmes de recherche d'actifs utilisés par Hadrian emploient les meilleures pratiques et des techniques propriétaires. L'équipe de développement interne met continuellement à jour la technologie pour identifier de nouvelles classes d'actifs et améliorer l'automatisation.

Coûts élevés des assurances cyber

Lors de la négociation des ajustements de prime avec une organisation, les fournisseurs d'assurance cybernétique prennent en compte de nombreux facteurs. Cependant, les organisations manquent de visibilité sur la posture de sécurité de leurs pairs ou d'elles-mêmes.

Sans accès à des preuves crédibles sur la solidité de la posture de sécurité de l'organisation ou des benchmarks industriels, les primes d'assurance cyber sont estimées à 1 500 $ par an par million de dollars de dommages.

Réduction des primes d'assurance

Hadrian permet aux organisations de réaliser des économies grâce à des termes et conditions préférés pour leur assurance cyber. En fournissant des preuves mesurables de la réduction du risque de violation, les organisations sont équipées pour négocier avec les fournisseurs d'assurance.

La plateforme permet également aux organisations de comparer leur sécurité à celle de leurs pairs, leur permettant de comprendre leur posture de sécurité relative et leur réactivité face aux menaces.

Perte de revenus et dommages

Une violation ou une interruption de service peut avoir un impact matériel sur le résultat net d'une organisation. Les coûts subséquents incluent la remédiation, le temps d'arrêt, la perte de productivité, les amendes légales et les dommages à la marque.

Les amendes réglementaires, telles que les pénalités RGPD, peuvent être sévères, imposant potentiellement des charges financières significatives aux organisations. De plus, les organisations peuvent également faire face à un examen accru de la part des régulateurs.

Résilience accrue

Hadrian permet aux organisations de réduire leur exposition aux risques avec des étapes claires et actionnables. Cela réduit non seulement la probabilité d'une violation, mais réduit également l'impact potentiel que celle-ci pourrait avoir.

Selon le rapport d'IBM sur le Coût d'une Violation de Données, 35 % des organisations investissent dans des tests de sécurité offensive après une violation. En investissant tôt, les organisations peuvent prendre de l'avance et réduire significativement la probabilité.

Équipes de sécurité en silos

Slow security testing practices are not fit for purpose in today's fast paced development cycles. Penetration tests can take a month to plan, 2 months to perform and then several weeks for the report to be compiled. This is incompatible with development teams that work in 2 week sprint.

Existing tools to perform security assessments are complex. Not only are they difficult to configure and use, the results often contain false positives and are difficult for non-security personnel to understand and act upon.

Flux de travail collaboratifs et rationalisés

Hadrian streamlines the attack surface management process, enabling security operations to maintain a secure cyber environment. The platform’s automated penetration testing capabilities identify exploitable risks in real-time, providing development teams with near-instant feedback.

Orchestrator AI is built to simplify offensive security workflows by autonomously validating results to remove false-positives. Hadrian also provides step-by-step instructions to enable remediating teams to immediately take action.

Applications tierces et oubliées

Découvrir les vulnérabilités dans les logiciels tiers devient un défi pour les organisations sans une liste d'inventaire à jour et précise. L'absence de visibilité sur les surfaces d'attaque externes et les lacunes de sécurité.

Le manque de visibilité pose un problème significatif. Par exemple, un environnement de préproduction peut avoir été créé pour tester la fonctionnalité d'une nouvelle fonctionnalité mais n'a pas été déclassé. De telles applications négligées échouent souvent à répondre aux normes de sécurité.

Visibilité de la chaîne d'approvisionnement

Les sondes de Hadrian sont capables d'identifier plus de 10 000 applications SaaS et des milliers de paquets logiciels et versions, assurant une identification complète des applications.

En scannant continuellement internet, la plateforme de Hadrian examine la technologie, les versions et les configurations pour identifier les menaces de sécurité potentielles. Ce processus permet à Hadrian de révéler la posture de votre organisation et d'évaluer l'impact d'un compromis dans les logiciels tiers.

Abus de marque et phishing

Le nombre étendu de sous-domaines et la nature dynamique de l'infrastructure DNS posent des défis pour la surveillance. Les sous-domaines peuvent facilement passer inaperçus, les rendant susceptibles de tentatives de prise de contrôle et de compromission de l'infrastructure.

Des sous-domaines non réclamés ou mal gérés peuvent servir de point d'entrée pour les acteurs de menaces, entraînant des dommages potentiels à la marque, une perte de confiance des clients et des violations de données. Par exemple, les attaquants peuvent exploiter un sous-domaine pour voler des cookies d'authentification.

Construire une marque de confiance

Hadrian prévient les dommages à la marque en surveillant les vulnérabilités des sous-domaines susceptibles de prises de contrôle. La plateforme scanne continuellement l'infrastructure DNS pour identifier les risques émergents.

La plateforme alerte instantanément les équipes de sécurité, permettant une remédiation proactive et empêchant les sous-domaines d'être pris pour être utilisés dans une campagne de phishing. Une remédiation rapide élimine le risque que les clients, employés et partenaires rencontrent des sites de phishing malveillants.

À propos de Hadrian

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 découvrent et valident les risques de manière autonome.

Notre solution

La plateforme de Hadrian combine la découverte de la surface d'attaque, les tests de pénétration automatisés et les technologies de gestion de l'exposition aux menaces dans une plateforme basée sur le cloud et sans agent. La plateforme est alimentée par l'Orchestrateur IA, qui émule les techniques et comportements d'un véritable acteur de menace, pour fournir une détection continue 24x7 des menaces orientées internet et éliminer de manière autonome les faux positifs.

L'Orchestrateur IA utilise sa connaissance de votre environnement pour tester les risques exploitables du Top Dix OWASP, les vulnérabilités connues et de jour zéro, ainsi que les services exposés et mal configurés. Les scans sont enchaînés pour simuler des attaques multidimensionnelles complexes. La technologie de pointe est constamment mise à jour et améliorée par l'équipe de hackers Hadrian.

+200	+1.2m	40%
entreprises protégées	actifs sécurisés	temps moyen de résolution plus rapide

Approuvé par

ABN·AMRO · SHV ENERGY · macmillan education

WeatherTech · LEROY MERLIN · LOTTOMatica

RITUALS... · BIOLANDES · nedap

> “Ce qui est excitant avec ce que fait Hadrian, c'est qu'ils ont résolu un casse-tête apparemment impossible : trouver des faiblesses dans un réseau complexe avec un niveau de détail semblable à celui d'un humain, à grande échelle, de l'extérieur et de manière continue. Ce qui prend habituellement à une équipe dédiée d'ingénieurs en sécurité quelques semaines à découvrir pour un système, ils peuvent le faire en quelques minutes pour des milliers de systèmes.”
>
> **Tiago Teles, Security Lead - ABN AMRO**