HADRIAN

La fiabilité de votre programme de gestion des vulnérabilités dépend de son maillon le plus faible.

La plupart des RSSI savent que leur programme n'est pas encore au niveau attendu. La difficulté consiste toutefois à identifier précisément l'élément qui freine l'ensemble du dispositif, et à comprendre comment son amélioration pourrait transformer radicalement la vitesse de remédiation, la fiabilité des validations et la visibilité auprès de la direction.

Le problème est rarement une question de ressources. Quel que soit leur niveau de maturité, les entreprises sont confrontées à la même frustration : des outils sont déployés et des processus définis, pourtant le retard dans la remédiation ne cesse d'augmenter, les résultats s'accumulent plus vite qu'il est possible de les valider, et le conseil d'administration exige des réponses que le programme n'est pas encore capable d'apporter.

La raison est structurelle. La gestion des vulnérabilités externes comprend quatre modes de fonctionnement distincts. La plupart des entreprises sont plus performantes dans certains domaines que dans d'autres. Le maillon le plus faible limite le potentiel de tout le reste du programme. Tant que cette difficulté n'est pas identifiée et réglée, toutes les améliorations seront vaines, quels que soient les autres changements apportés.

Définition du modèle

Le modèle de maturité en matière d'exposition de Hadrian identifie quatre niveaux de gestion des vulnérabilités externes, allant d'une approche réactive et sans identification à une approche continue et autonome. Chaque niveau correspond à un mode de fonctionnement identifiable qui repose sur des schémas de programme réels, et non à un cadre théorique. Le modèle s'appuie sur sept dimensions opérationnelles pour vous indiquer votre situation réelle et les obstacles opérationnels qui vous freinent.

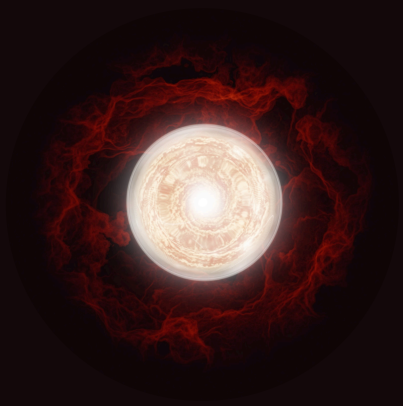
L'IMPORTANCE DE LA MONTÉE EN MATURITÉ

NIVEAU 1 À 2

Le MTTR passe de plus de 90 jours à 45. La couverture passe de 20 % à 40-60 %

NIVEAU 2 À 3

Le taux de résultats positifs réels atteint 40-60 %. Le taux de conformité au SLA atteint 60-80 %. Le MTTR est réduit à 15-45 jours.



NIVEAU 3 À 4

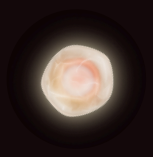
La couverture dépasse 95 %. Les vulnérabilités critiques sont corrigées dans les 48 heures. Les failles identifiées sont confirmées en quelques heures, et non en quelques jours.

LES MENACES N'ATTENDENT PAS

Le délai moyen entre la découverte d'une vulnérabilité et son exploitation active est passé de 32 à 5 jours. Près d'une faille sur trois est désormais exploitée le jour même de sa découverte, voire avant.

La plupart des programmes de sécurité s'articulent autour de cycles de tri hebdomadaires et de tests trimestriels. Le décalage entre la rapidité des attaquants et la maturité des programmes n'est pas un risque pour demain, c'est une réalité d'aujourd'hui.

Les quatre niveaux



NIVEAU 1

Navigation à vue

Les vulnérabilités sont détectées de manière réactive. Les responsabilités ne sont pas clairement définies. La file d'attente des mesures correctives s'allonge plus vite qu'elle ne diminue. L'équipe consacre la plupart de ses ressources à traiter des résultats qui s'avèrent sans importance.

- Détection réactive
- Absence de responsabilité systématique pour les actifs
- Tri basé sur le CVSS
- Rapports axés sur la conformité

NIVEAU 2

Périmètre défini, plus d'espoir

Le programme est structuré et la couverture s'améliore. La validation reste le point faible : l'exploitabilité est supposée à partir des scores de gravité au lieu d'être confirmée. Le MTTR se situe entre 45 et 90 jours.

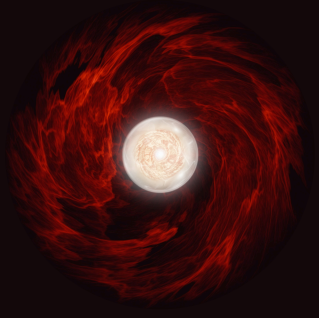
- Tests d'intrusion planifiés
- Couverture des actifs connus
- Analyse manuelle de l'exploitabilité
- Indicateurs basés sur l'activité

NIVEAU 3

Corrélation des données

Les résultats sont validés avant d'être intégrés dans la file d'attente. Le taux de résultats positifs réels atteint 40-60 %. Le MTTR est réduit à 15-45 jours. La difficulté réside dans la mise en relation des résultats pour obtenir une vue d'ensemble complète de l'attaque sans intervention manuelle importante.

- Surveillance continue
- Validation automatisée
- Traitement intégré de la remédiation
- Mesure des risques exploitables



NIVEAU 4

Visibilité totale

L'identification est continue, la validation est autonome et la direction dispose en temps réel des données sur la sécurité. La couverture dépasse 95 %. Les vulnérabilités critiques sont corrigées dans les 48 heures. Les nouvelles failles sont confirmées en quelques heures.

- Émulation autonome
- Visibilité en temps réel sur la posture de sécurité
- Définition prédictive des priorités
- Rapports en direct sur le tableau de bord

LA PLUPART DES PROGRAMMES SONT LIMITÉS PAR UN SEUL POINT FAIBLE.

L'auto-évaluation interactive analyse votre programme de manière indépendante pour chacun des sept domaines, identifie vos obstacles opérationnels et génère un plan d'action que votre équipe peut mettre en œuvre immédiatement dans chaque niveau. Cela ne vous prendra que 5 minutes.

RÉALISER L'AUTO-ÉVALUATION SUR HADRIAN.IO

À PROPOS D'HADRIAN

Hadrian est une plateforme de sécurité offensive qui identifie et valide les vulnérabilités externes à la manière d'un attaquant : elle part d'un périmètre non prédéfini, suit les chemins d'attaque partout où ils mènent et vérifie que chaque résultat est réel avant de les transmettre à votre équipe. Reconnue dans le « Hype Cycle » de Gartner consacré aux opérations de sécurité, ainsi que par GigaOm et Frost & Sullivan.

POUR EN SAVOIR PLUS : HADRIAN.IO

Frost & Sullivan Best Practices Awards

GigaOm Radar Report Leader 2025

Gartner Peer Insights 4.9/5 ★

AICPA SOC · ISO 27001

RECOMMANDÉ PAR PLUS DE 300 GRANDES ENTREPRISES

NBC · amadeus · McKESSON · BLINQX · Crédit Agricole · Leroy Merlin · SHV

ABN·AMRO · London Business School · RITUALS... · SIEMENS energy · LOTTOMATICA · FP Francisco Partners · CHRISTIE'S

BIOLANDES · WeatherTech · BLINQX · DAMEN · jamf · exact

ICT GROUP · nedap · celio* · Inova · XM Cyber · AROMA360