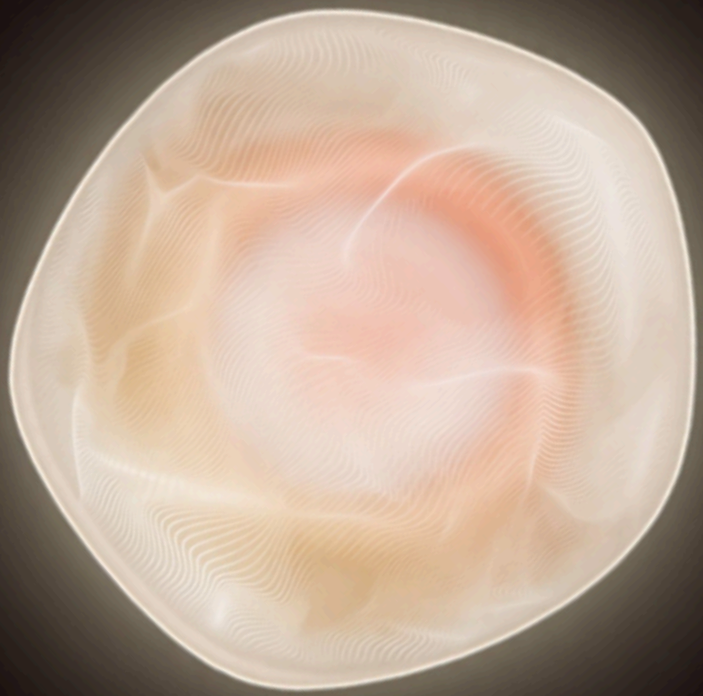
HADRIAN

EXPOSITION EXTERNE MODÈLE DE MATURITÉ



Où en est votre programme de gestion de l'exposition aux menaces aujourd'hui, et à quoi ressemble concrètement une évolution significative ?

LE PROBLÈME D'EXPOSITION QUE LES PROGRAMMES NE PARVIENNENT PAS À RÉSOUDRE

La plupart des entreprises ont investi massivement dans des outils de sécurité. Elles utilisent des analyses de vulnérabilité, exploitent des plateformes SIEM, réalisent des tests d'intrusion annuels ou trimestriels et gèrent un programme de gestion des vulnérabilités avec des responsables désignés et des accords sur le niveau de service (SLA). Pourtant, le même schéma continue de se répéter : les vulnérabilités exploitables persistent, les remédiations en attente s'accumulent rapidement, et lorsqu'un incident survient, la faille qui l'a rendu possible figurait souvent dans un rapport depuis des mois.

Le problème ne vient pas d'un manque de mesures de sécurité, mais à l'absence d'une structure de programme qui relie les activités aux résultats. L'analyse produit des résultats. Les résultats génèrent des tickets. Les tickets sont traités et fermés (ou non). Mais la vraie question qui compte (à savoir, la vulnérabilité exploitable de l'entreprise est-elle réellement réduite ?) reste souvent sans réponse.

C'est précisément cette faille que le modèle de maturité de l'exposition externe vise à corriger. Il décrit quatre modes de fonctionnement distincts, chacun étant défini non pas par les outils disponibles, mais par la manière dont une entreprise identifie une vulnérabilité, confirme son existence et la corrige avant qu'un attaquant agisse. Ce modèle offre aux responsables de la sécurité un cadre précis pour évaluer l'état actuel de leur programme, identifier les obstacles structurels qui le bloque et déterminer les changements nécessaires pour évoluer.

Comment cela s'inscrit dans le cadre de la CTEM

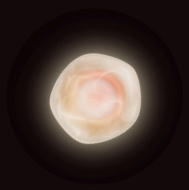
La gestion continue de l'exposition aux menaces (CTEM) est un modèle en cinq phases, élaboré par Gartner, qui fournit une structure permettant de passer d'une gestion réactive des vulnérabilités à une réduction continue de l'exposition, axée sur les résultats. Les phases sont les suivantes : le périmètre, l'identification, la priorisation, la validation, la mise en place des mesures correctives. Ce modèle correspond directement aux niveaux de maturité de la CTEM : les entreprises des niveaux 1 et 2 en sont généralement aux premières phases, tandis que celles des niveaux 3 et 4 ont terminé le cycle en passant par les étapes de validation et de mobilisation. La phase où la plupart des déploiements de la CTEM se heurtent à un blocage est celle de la validation : il s'agit de confirmer que les résultats mis en évidence correspondent à un risque réellement exploitable, et non à une menace purement théorique. C'est le point d'inflexion structurel autour duquel ce modèle s'articule.

POURQUOI LA PROGRESSION EST-ELLE IMPORTANTE ?

L'écart entre les niveaux 1 et 4 n'est pas une question de ressources, c'est une question de structure : comment une entreprise détecte une vulnérabilité, vérifie qu'elle est bien réelle et la corrige avant qu'un attaquant passe à l'action.

Ce que l'évolution apporte concrètement

The gap between Stage 1 and Stage 4 is not a matter of resources. It is a matter of structure: how an organisation discovers exposure, confirms it is real, and closes it before an attacker can act.



NIVEAU 1 → NIVEAU 2

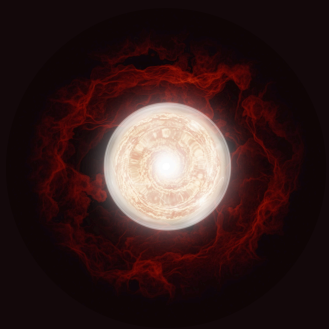
Navigation à vue → Périmètre défini, plus d'espoir

La surface de surveillance passe de moins de 20 % à 40-60 %. Les taux de résultats positifs réels passent de moins de 10 % à 15-25 %. Cela signifie que le nombre d'alertes nécessitant une inspection passe de moins de 1 sur 10 à 1 sur 4 à 6. Le temps de remédiation moyen passe de plus de 90 jours à 45-90 jours. Conséquence directe : l'équipe de sécurité ne consacre plus la plupart de son temps à des questions qui se révèlent sans incidence.

NIVEAU 2 → NIVEAU 3

Périmètre défini, plus d'espoir → Corrélation des données

La couverture atteint 75-90 % de la surface. Les taux de résultats positifs réels grimpent à 40-60 %, ce qui signifie que près de la moitié des vulnérabilités identifiées sont confirmées comme étant exploitables avant même d'avoir été examinées. Le MTTR est réduit à 15-45 jours. Le taux de conformité au SLA atteint 60-80 %. Les remédiations en attente sont moins nombreuses et plus précises : le nombre total de problèmes identifiés diminue, le niveau de fiabilité pour chacun d'entre eux augmente, et on observe une réduction notable des vulnérabilités exploitables, au-delà de la simple fermeture des tickets.



NIVEAU 3 → NIVEAU 4

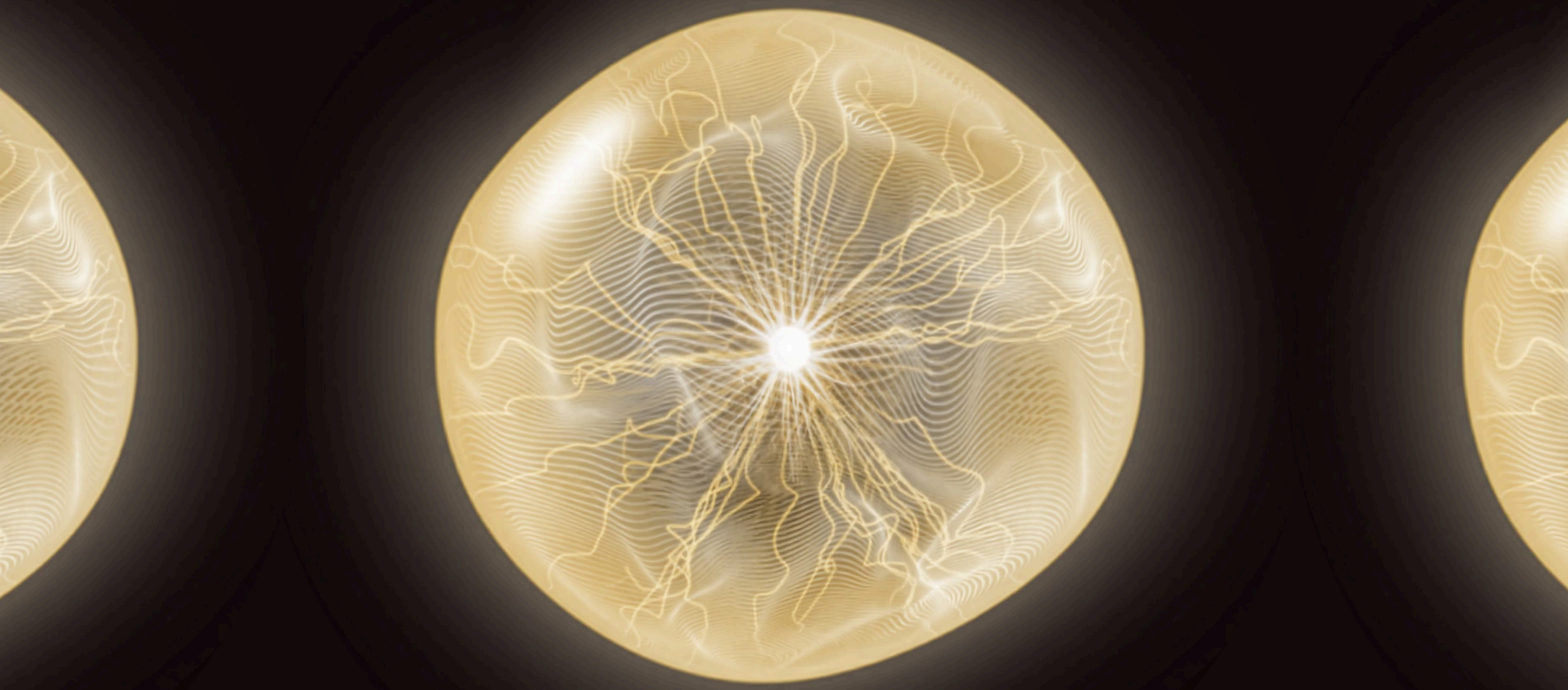
Corrélation des données → Visibilité totale

La couverture dépasse 95 %. Le taux de résultats positifs réel dépasse 70 %. Le MTTR passe sous la barre des 7 jours ; les vulnérabilités critiques sont corrigées dans les 48 heures. Le taux de conformité au SLA dépasse 90 %. Critère le plus important : lorsqu'une nouvelle faille est découverte, l'entreprise peut vérifier si elle est exposée en quelques heures, contre plusieurs jours. Au niveau 3, cette vérification nécessitait une réunion d'équipe et une analyse manuelle. Au niveau 4, le programme y répond automatiquement.

Utilisez ces données comme un outil de diagnostic, une feuille de route ou un langage commun avec la direction. Elles ne préconisent aucun ensemble d'outils ni aucun calendrier précis. Aucune entreprise n'est tenue d'atteindre le niveau 4 pour chaque actif. La vraie question n'est pas de savoir où nous en sommes, mais plutôt de savoir si le programme fonctionne au niveau requis par le profil de risque.

SECTION 2

APERÇU DU MODÈLE



Knowing where your programme stands is the starting point for meaningful advancement. This section will give you a picture of the specific capability gaps and measurable outcomes that define each stage.

Tableau d'analyse

Pour chaque critère, cochez la colonne qui décrit le plus fidèlement votre programme actuel. Si vos réponses se concentrent dans une seule colonne, il s'agit de votre niveau actuel. Si elles sont dispersées, votre niveau de base correspond à la colonne la plus à gauche que vous avez cochée.

CRITÈRE	NIVEAU 1: NAVIGATION À VUE	NIVEAU 2: PÉRIMÈTRE DÉFINI, PLUS D'ESPOIR	NIVEAU 3: CORRÉLATION DES DONNÉES	NIVEAU 4: VISIBILITÉ TOTALE
Rythme opérationnel À quelle fréquence votre programme évalue-t-il sa vulnérabilité ?	DE MANIÈRE RÉACTIVE	DE MANIÈRE PÉRIODIQUE	EN CONTINU	AUTONOME
Rapport au risque Dans quelle mesure comprenez-vous votre vulnérabilité réelle ?	VULNÉRABLE	CONSCIENT	VALIDÉ	PROACTIF
Stratégie de sécurité Comment votre programme se positionne-t-il face aux attaquants ?	DE MANIÈRE RÉACTIVE	DE MANIÈRE STRUCTURÉE	DE MANIÈRE PROACTIVE	DE MANIÈRE PRÉDICTIVE
Approche de validation Comment votre programme évalue-t-il l'efficacité de vos contrôles ?	SUPPOSÉE	TESTÉE	VALIDÉE	EN CONTINU

La matrice des capacités

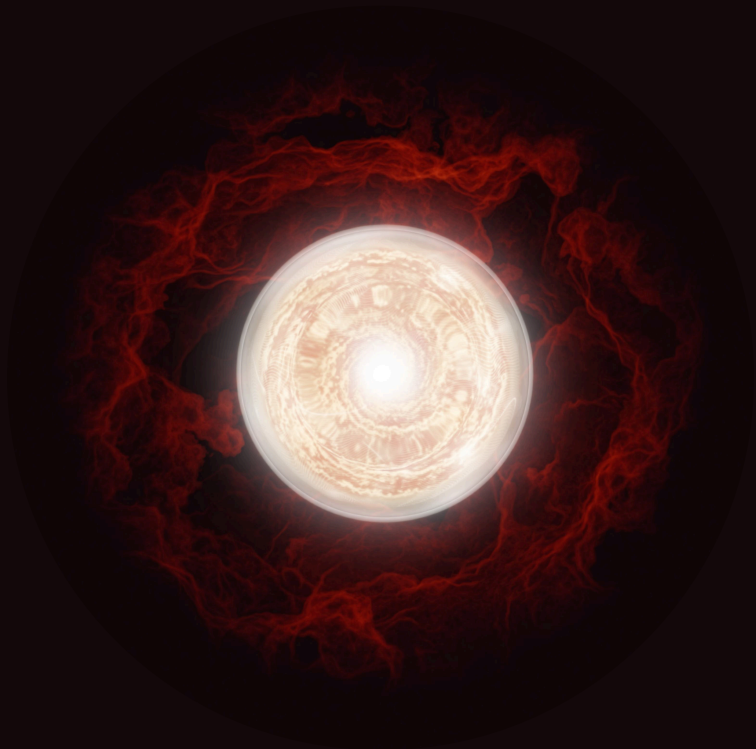
Cinq dimensions opérationnelles, quatre niveaux. Utilisez-la pour identifier la dimension qui constitue votre facteur limitant.

CAPABILITY	NIVEAU 1: NAVIGATION À VUE	NIVEAU 2: PÉRIMÈTRE DÉFINI, PLUS D'ESPOIR	NIVEAU 3: CORRÉLATION DES DONNÉES	NIVEAU 4: VISIBILITÉ TOTALE
Modèle opérationnel	Approche réactive ; vulnérabilités identifiées à la suite d'incidents ou d'audits	Programme structuré ; responsabilités clairement définies ; mise en place des phases de la CTEM	Écart comblé ; les résultats de la validation définissent la remédiation	Approche offensive par défaut ; capacité d'adaptation ; intervention manuelle réduite au minimum
Identification	Inventaire statique incomplet ; analyse périodique des actifs connus	EASM déployée ; cloud, SaaS, API et solutions tierces pris en compte	Surveillance continue ; détection des anomalies quasiment en temps réel	Capacité d'adaptation ; corrèle automatiquement l'identité, l'infrastructure et les solutions SaaS
Priorisation	Scores CVSS et fournisseurs ; contexte métier limité	Basé sur le risque avec intégration de la criticité métier	Contexte d'exploitabilité et de chemin d'attaque ; moins d'alertes, mais de plus haute confiance	Prédictif et sensible au contexte ; les priorités évoluent de manière dynamique
Validation	Tests d'intrusion annuels ou ponctuels ; exploitabilité supposée, non confirmée	Tests périodiques à partir de scénarios dans des périmètres définis	Validation automatisée continue ; élimination des périodes sans visibilité	Émulation d'adversaire autonome ; adaptation des chaînes d'attaque aux changements
Automatisation	Manuelle, basée sur des tickets ; outils cloisonnés	Flux de travail intégrés ; transferts standardisés	La validation déclenche la remédiation ; intégrations SOC/IT actives	Largement autonome ; les équipes se concentrent sur les décisions stratégiques

Indicateurs de référence quantitatifs

Plages de performance indicatives par niveau. Utilisez-les pour orienter votre stratégie, et non comme des seuils de réussite ou d'échec.

INDICATEURS	NIVEAU 1: NAVIGATION À VUE	NIVEAU 2: PÉRIMÈTRE DÉFINI, PLUS D'ESPOIR	NIVEAU 3: CORRÉLATION DES DONNÉES	NIVEAU 4: VISIBILITÉ TOTALE
Surface d'attaque sous surveillance continue	< 20%	40–60%	75–90%	> 95%
Taux de résultats positifs réels	< 10%	15–25%	40–60%	> 70%
Temps moyen de remédiation (MTTR)	> 90 jours	45–90 jours	15–45 jours	< 7 jours (critique : < 48h)
Conformité au SLA	< 20%	< 40%	60–80%	> 90%
Résultats validés comme exploitables avant escalade	Rarement	De manière sélective	De manière systématique	En continu et automatiquement



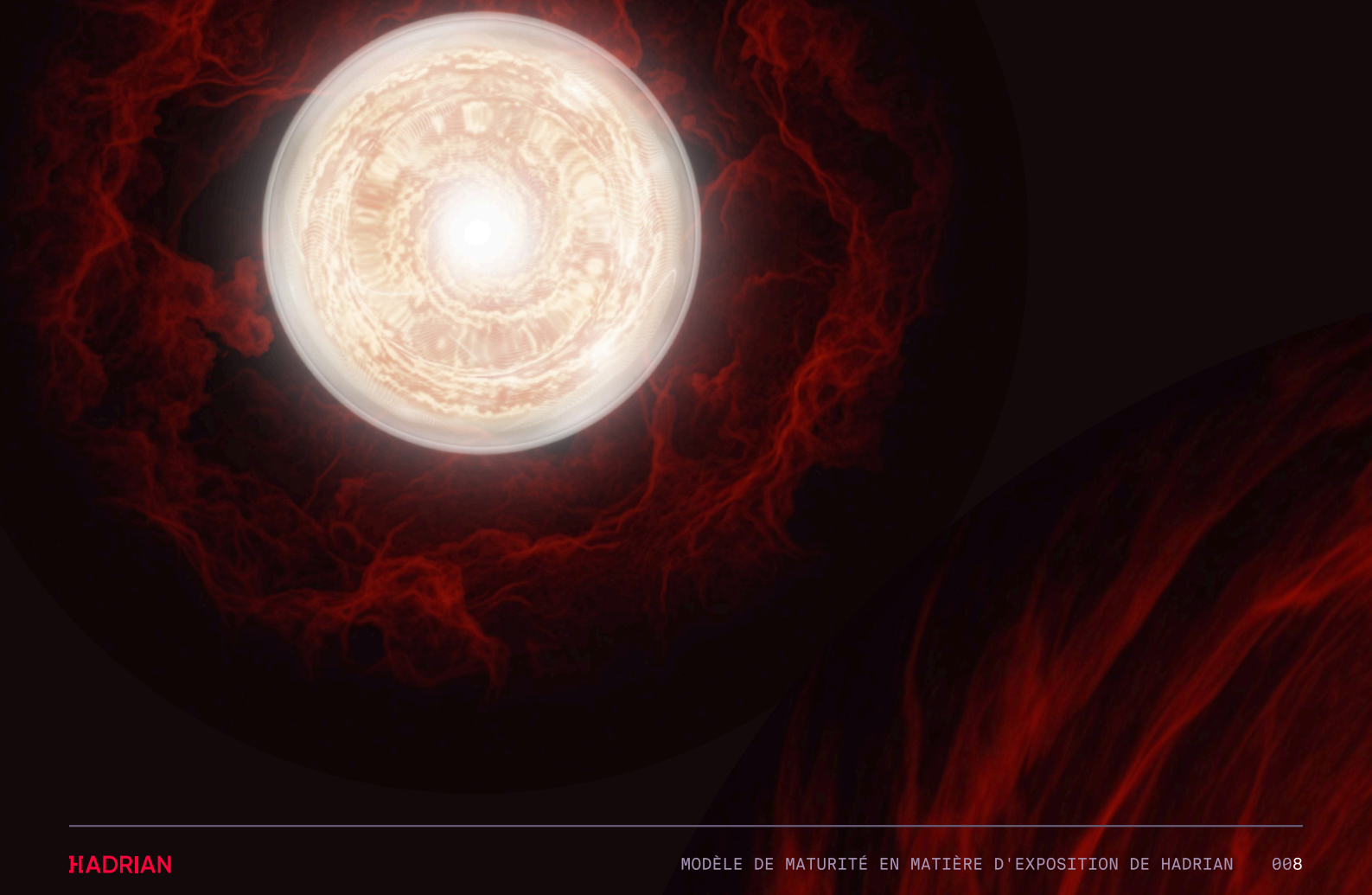
ÉVALUEZ-VOUS :

Réalisez l'auto-évaluation interactive pour obtenir un profil de maturité personnalisé et un plan d'action

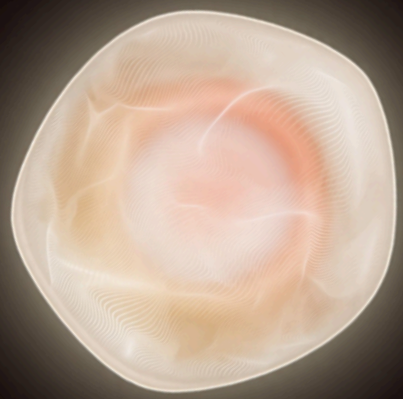
DÉCOUVREZ VOTRE NIVEAU DE MATURITÉ

LES QUATRE NIVEAUX

Chaque niveau correspond à un mode de fonctionnement identifiable, et non à un score ou à une note. Considérez-les comme des représentations du fonctionnement réel des entreprises. Si une description vous met mal à l'aise, c'est probablement celle qui correspond à votre situation.



NIVEAU 1



NAVIGATION À VUE

« On ne se rend compte des failles de sécurité que lorsque les problèmes surviennent. »

L'appellation parle d'elle-même. L'entreprise n'a aucune image fiable de sa surface d'attaque externe. Les actifs apparaissent dans les discussions après les incidents, pas avant. L'équipe de sécurité sait qu'il lui manque des éléments ; mais elle ignore de quoi il s'agit, où ils se trouvent, et quelle est leur importance. Des analyses sont lancées, mais elles aboutissent à une liste de menaces à laquelle personne ne fait vraiment confiance et qui s'allonge plus vite qu'elle ne peut être traitée.

Ce qui distingue le niveau 1 du niveau 2, ce ne sont pas les outils. À ce niveau, la plupart des entreprises disposent déjà de programmes de détection, de systèmes SIEM et de processus de gestion des tickets. Ce qui leur manque, c'est une structure : il n'y a pas de cadence systématique pour l'identification des vulnérabilités, pas de modèle de responsabilité clairement défini, ni de méthode systématique pour vérifier si les résultats détectés constituent un risque réel. L'activité existe. Le programme, non.

Ce qu'en disent les équipes

« On ne fait qu'éteindre des incendies. On ne peut jamais anticiper. »

« Le rapport de test d'intrusion vient d'arriver, et il nous reste encore la moitié des problèmes de l'année dernière à régler. »

« Je ne sais même pas combien nous avons d'actifs exposés sur Internet. Personne ne le sait. »

À quoi cela ressemble sur le plan opérationnel

Les réunions sur la sécurité sont dominées par l'incident le plus récent ou les conclusions d'un audit. Le compte rendu du RSSI au conseil d'administration porte principalement sur l'état de conformité, plutôt que sur les risques d'exposition. Lorsqu'une nouvelle CVE critique est signalée, la priorité est de se demander si on utilise ce logiciel. Et personne ne connaît vraiment la réponse. Les discussions sur la remédiation commencent plus souvent par « qui est responsable de cette équipe ? » plutôt que par « quel est le niveau de vulnérabilité ? ». Le rapport de test d'intrusion datant d'il y a huit mois est toujours ouvert dans un tableur dont les recommandations n'ont jamais été pleinement mises en œuvre.

Ce qui freine les entreprises

La principale raison n'est pas une question de budget. C'est que l'entreprise a défini la sécurité comme une fonction de conformité plutôt que comme une fonction de gestion des risques, et la conformité n'exige pas de savoir ce qui est vulnérable, mais seulement ce qui est documenté. Cela crée un plafond de verre structurel : le programme produit des preuves d'activité plutôt que des preuves de réduction du risque, et la direction ne sait pas encore faire la distinction.

L'obstacle opérationnel du niveau 1 réside dans l'effondrement du rapport signal/bruit. Les programmes de détection génèrent des milliers de résultats sans aucun mécanisme permettant de distinguer le risque réel du bruit de fond. Résultat : l'ensemble des capacités de l'équipe est consacré au tri, et non à la remédiation. Le volume donne l'impression que le travail est fait, mais il ne garantit en rien la sécurité.

La responsabilité est le troisième obstacle. La vulnérabilité se situe à la croisée de la sécurité, de l'informatique et de l'ingénierie. Lorsque personne n'a une vue globale de la situation, rien n'est considéré comme urgent tant qu'il n'y a pas de problème.

Le point de bascule

Les entreprises sont prêtes évoluer lorsqu'un élément rend le problème indéniable, généralement un incident qui a révélé l'existence d'un actif dont personne n'avait connaissance, ou une question posée par le conseil d'administration qui a mis en évidence l'écart entre la stratégie annoncée et la stratégie réelle. Le passage d'une approche axée sur la conformité à une approche axée sur les risques nécessite souvent un défenseur en interne : quelqu'un capable d'orienter la discussion non pas vers « nous avons besoin de plus d'outils », mais vers « nous devons savoir à quoi nous sommes réellement exposés ».

Changements nécessaires sur le plan structurel

La condition préalable au niveau 2 n'est pas l'achat d'un nouvel outil. C'est une question de responsabilité. Quelqu'un doit être responsable de tout l'inventaire des actifs externes, et pas seulement de la sécurité des actifs connus. Une fois cette responsabilité établie, les structures nécessaires suivent : identification continue des actifs au-delà du périmètre prédéfini, définition des priorités fondée sur les risques en tenant compte du contexte métier parallèlement aux scores de gravité, et accords sur le niveau de service (SLA) définis qui sont réellement appliqués et ne restent pas de simples objectifs.

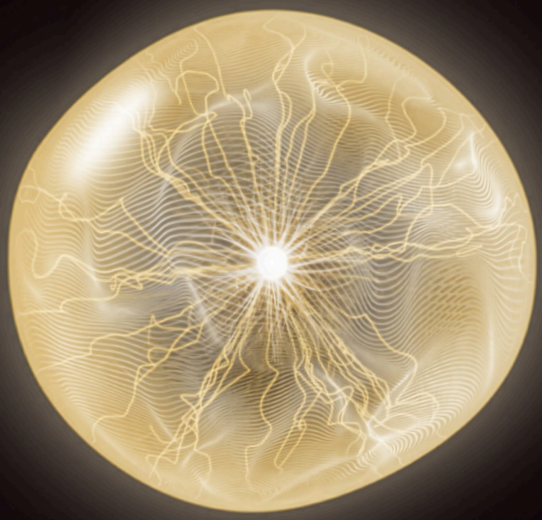
Fonctionnalités permettant cette transition

- Gestion de la surface d'attaque externe permettant d'identifier les actifs en dehors de l'inventaire prédéfini : cloud, SaaS, filiales, tiers
- Définition des priorités en fonction des risques, tenant compte de la criticité métier et de l'accessibilité, au-delà du simple score CVSS
- Flux de travail d'assignation des actifs, permettant de lier les actifs identifiés aux équipes responsables

TÉLÉCHARGER LE PLAN D'ÉVOLUTION DU NIVEAU 1 AU NIVEAU 2

NIVEAU 2

PÉRIMÈTRE DÉFINI, PLUS D'ESPOIR



« Nous en savons plus qu'avant. Mais nous ne sommes pas certains que ce soit assez. »

Les organisations de niveau 2 ont fourni des efforts concrets. Il existe un programme officiel de gestion des vulnérabilités. Les principaux actifs sont répertoriés. Les tests sont effectués selon un calendrier précis et non plus uniquement après des incidents. L'équipe de sécurité dispose d'une place à la table des décisions et d'un mandat clairement défini. Le RSSI est en mesure de produire sans difficulté un rapport sur la posture de sécurité.

Cette appellation reflète à la fois les progrès accomplis et les limites qui subsistent. Le périmètre est élargi : plus d'actifs, une couverture de test plus étendue, des responsabilités mieux définies. Et il y a un réel espoir : l'espoir que les actifs connus soient bien les plus importants, l'espoir que les tests d'intrusion trimestriels aient détecté ce qui est essentiel, l'espoir que la vulnérabilité corresponde globalement à la gravité. Cet espoir n'est pas infondé. Mais cela reste un espoir, pas une preuve. Le programme est structuré ; il n'a pas encore été validé.

Ce qu'en disent les équipes

« Les résultats du dernier test d'intrusion sont déjà obsolètes au moment où le cycle suivant est lancé. »

« Nous couvrons bien les actifs dont nous avons connaissance. Le problème, ce sont ceux que nous ignorons. »

« En théorie, nous adoptons une approche fondée sur les risques. Dans la pratique, nous continuons à traiter les vulnérabilités notées 9 ou 10 sur l'échelle CVSS. »

À quoi cela ressemble sur le plan opérationnel

L'équipe de sécurité suit un calendrier bien établi : tests d'intrusion trimestriels, analyses régulières des vulnérabilités, file d'attente des tickets avec des responsables désignés. Les rapports destinés au conseil d'administration ont évolué : ils ne se limitent plus à l'état de conformité, mais traitent désormais de l'exposition actuelle aux vulnérabilités. Lorsqu'une nouvelle CVE est publiée, un processus de vérification est en place, mais il est manuel et plus lent qu'espéré.

Ce qui freine les entreprises

Le principal obstacle au niveau 2 réside dans le décalage entre la fréquence des tests et la vitesse d'évolution de l'environnement. Les tests d'intrusion trimestriels ont été conçus pour des environnements qui évoluaient tous les trois mois. Aujourd'hui, la plupart des environnements professionnels changent quotidiennement. Le programme n'est pas défaillant, mais il n'est pas adapté au rythme auquel le problème évolue.

L'obstacle opérationnel du niveau 2 réside dans la validation manuelle. Pour confirmer qu'une vulnérabilité est réellement exploitable, une inspection humaine est nécessaire. Lorsque cette étape ne suit pas le rythme, les files d'attente de remédiations se remplissent de résultats non validés, et les équipes ont recours à des méthodes empiriques informelles : tout ce qui dépasse un score CVSS de 8 est considéré comme exploitable. C'est plus rapide. C'est également beaucoup moins précis, et cela ne permet ni de réduire le retard accumulé ni d'améliorer la confiance dans ce qui reste à faire.

Cette méthode d'évaluation ne fait qu'aggraver ces deux problèmes. La plupart des programmes de niveau 2 surveillent la couverture et l'activité : vulnérabilités identifiées, vulnérabilités corrigées, conformité au SLA. Ces indicateurs donnent l'impression qu'il y a du progrès, mais ils ne répondent pas à la question qui intéresse vraiment la direction : nos vulnérabilités exploitables sont-elles moins nombreuses ?

Le point de bascule

Le déclic est généralement l'identification d'une vulnérabilité qui aurait dû être détectée plus tôt. Une faille exploitable découverte entre deux cycles de test, lors d'une évaluation ponctuelle ou par un consultant externe. La question qui s'ensuit (à savoir, depuis combien de temps cette faille existe-t-elle ?) est souvent le point de départ qui permet de reconnaître que les validations périodiques ne suffisent plus. Il s'agit de savoir si l'entreprise est prête à passer de tests planifiés à une surveillance continue, et si la direction est disposée à financer les changements structurels que cela implique.

Changements nécessaires sur le plan structurel

Le passage du niveau 2 au niveau 3 nécessite de réduire l'écart qui existe entre la fréquence des tests et la vitesse d'évolution de l'environnement. Cela implique une surveillance externe continue capable de détecter les nouvelles vulnérabilités dès leur apparition, et pas seulement lors de la prochaine analyse programmée. Cela nécessite également de considérer la validation de la vulnérabilité comme une étape du processus de travail, et pas comme une inspection manuelle. Lorsque la validation d'une vulnérabilité réelle est automatisée et ne dépend plus d'une intervention humaine, l'obstacle saute au niveau du tri. Les indicateurs doivent eux aussi évoluer : le programme doit surveiller les risques exploitables éliminés, et pas seulement les incidents corrigés.

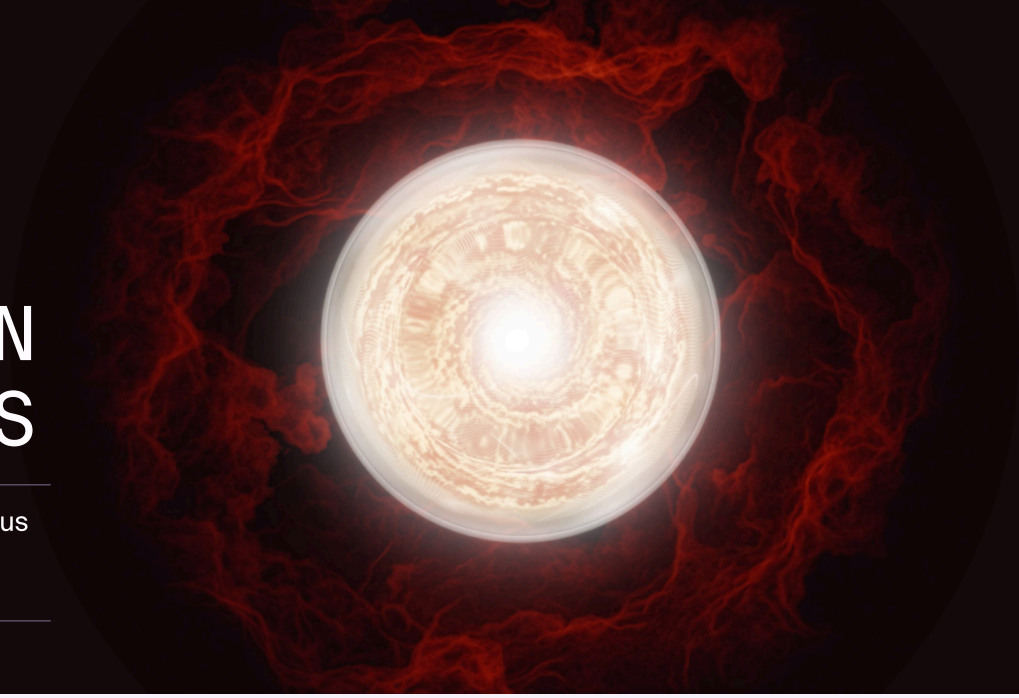
Fonctionnalités permettant cette transition

- Une surveillance continue de la surface d'attaque externe qui signale les nouveaux actifs et les changements survenus entre deux cycles de tests d'intrusion
- Une validation automatisée de la faille qui permet de confirmer quelles vulnérabilités sont réellement accessibles et testables
- Un processus intégré de remédiation afin que les vulnérabilités validées soient transmises au responsable compétent sans intervention manuelle

TÉLÉCHARGER LE PLAN D'ÉVOLUTION DU NIVEAU 2 AU NIVEAU 3

NIVEAU 3

CORRÉLATION DES DONNÉES



« Nous savons ce qui est exploitable. Nous commençons à voir comment tout cela s'articule. »

Le niveau 3 marque un véritable tournant opérationnel. La validation n'est plus périodique, elle est continue. Les périodes sans visibilité entre les cycles de test ont été en grande partie éliminées. La vulnérabilité n'est plus supposée sur la base des scores de gravité, elle est confirmée et les résultats sont transmis aux personnes responsables. Les processus de remédiation sont intégrés aux outils de sécurité, de sorte que les vulnérabilités validées sont automatiquement transmises au lieu de finir dans une boîte de réception partagée.

Le nom du programme en dit long sur cette nouveauté : pour la première fois, il ne se contente pas de répertorier les failles de manière isolée ; il les assemble pour obtenir une représentation de la manière dont un attaquant pourrait réellement agir. Chaque vulnérabilité validée est mise en correspondance avec des chemins d'attaque. La définition des priorités passe de « quelle est la note CVSS la plus élevée ? » à « quelles vulnérabilités peuvent être combinées pour causer des préjudices réels ? ». L'approche est fondamentalement différente. Le problème, c'est que créer et maintenir cette représentation nécessite encore une coordination humaine importante. Le programme identifie les éléments, mais établir des corrélations rapidement et à grande échelle reste un travail manuel.

Ce qu'en disent les équipes

« Nous savons ce qui est exploitable. La difficulté consiste à suivre le rythme effréné auquel l'environnement évolue. »

« Nos résultats sont validés avant d'être intégrés dans la file d'attente. La difficulté, c'est de faire des corrélations pour obtenir une vue d'ensemble complète de l'attaque. »

« Nous pouvons indiquer au conseil d'administration les vulnérabilités exploitables. Mais nous ne sommes pas encore en mesure de leur dire comment un attaquant pourrait combiner ces vulnérabilités. »

À quoi cela ressemble sur le plan opérationnel

Le quotidien de l'équipe de sécurité est transformé. Les résultats sont transmis après validation. Les tickets sont automatiquement envoyés aux personnes responsables. Pendant le tri, la question n'est plus de savoir si la menace est réelle, mais comment elle s'inscrit dans le schéma global de vulnérabilité. Le MTTR est mesuré activement, affiche une tendance à la baisse et il est défini en fonction du nombre de risques exploitables corrigés plutôt que du nombre de tickets.

Le reporting, les indicateurs pour le conseil d'administration et les KPI sont encore souvent construits autour de photos périodiques, parce que c'est ce que la direction a toujours demandé. Le conseil d'administration continue de vouloir un chiffre entre un et dix. Les KPI qui avaient du sens au stade 2 mesurent désormais les mauvaises choses, mais les faire évoluer nécessite une discussion que personne n'a encore priorisée. Pendant ce temps, l'équipe de sécurité fonctionne avec un niveau de précision pour lequel la structure de gouvernance n'a pas été conçue. Le RSSI peut vous dire ce qui est exposé. Il ne peut pas encore vous dire, suffisamment rapidement pour que cela ait un impact, ce qu'un attaquant pourrait exploiter.

Ce qui freine les entreprises

L'obstacle réside dans la capacité de gestion du flux de l'orchestration. Exécuter un scénario d'attaque complexe qui suit des chaînes d'attaques entre les systèmes, teste des chemins d'intrusion réalistes et s'adapte aux changements de l'environnement demande beaucoup de temps aux experts. Chaque résultat peut être validé en continu ; en revanche, la simulation de ce qu'un attaquant chevronné ferait réellement avec ces résultats reste un exercice manuel impliquant de nombreuses ressources. Le programme identifie les éléments. Faire les corrélations rapidement reste une tâche manuelle.

L'obstacle opérationnel du niveau 3 réside dans les capacités d'émulation. Le programme est capable de valider chaque résultat en continu, mais la traduction en une vue d'ensemble complète et en temps réel de la manière dont ces résultats s'assemblent pour former des chemins d'attaque exploitables nécessite encore une intervention manuelle pour chaque scénario. À mesure que les environnements gagnent en complexité, l'écart entre ce qui peut être validé et ce qui peut être émulé devient le facteur limitant.

Il y a également un décalage organisationnel. Les opérations se déroulent en continu, mais la gestion n'a pas suivi le rythme. Les rapports destinés à la direction, les indicateurs du conseil d'administration et les KPI s'appuient encore souvent sur des aperçus ponctuels plutôt que sur des données de sécurité en temps réel. Le programme génère plus d'informations que l'entreprise n'est capable d'en exploiter.

Le point de bascule

Les entreprises de niveau 3 sont prêtes à évoluer lorsqu'elles sont confrontées à une question précise à laquelle elles ne peuvent pas encore répondre rapidement : si une nouvelle catégorie de failles était révélée aujourd'hui, combien de temps nous faudrait-il pour vérifier si l'ensemble de notre surface est affecté ? Si la réponse honnête se compte en jours et pas en heures, l'écart entre la capacité de détection et la capacité d'émulation est devenu le facteur limitant. La question de la maturité repose sur deux piliers : la volonté de la direction d'investir pour combler cet écart, et la capacité de la gestion du programme à accepter un fonctionnement autonome.

Changements nécessaires sur le plan structurel

Le passage au niveau 4 nécessite de remplacer l'orchestration manuelle des scénarios d'attaques par une émulation automatisée qui s'adapte aux changements de l'environnement sans intervention humaine pour chaque scénario. Cela implique aussi de réduire l'écart qui existe entre les données opérationnelles en temps réel et la visibilité de la direction : des tableaux de bord sur la sécurité en temps réel créés directement à partir des résultats du programme, et non compilés périodiquement. Et cela nécessite une décision de gouvernance : pré-autoriser les protocoles de réponse rapide afin que, lorsqu'une nouvelle faille est découverte, le programme réagisse en quelques heures plutôt que d'attendre une réunion de tri.

Fonctionnalités permettant cette transition

- Une émulation d'adversaire automatisée qui s'adapte aux changements de l'environnement sans intervention manuelle pour chaque scénario
- Une évaluation en temps réel de la sécurité et des indicateurs de maturité présentés au conseil d'administration, directement créés à partir des données de programme en temps réel
- Une analyse continue de la chaîne d'attaque qui met en évidence comment les résultats validés s'assemblent pour former des chemins d'attaque exploitables

DOWNLOAD THE STAGE 3 TO 4 ADVANCEMENT PLAN

NIVEAU 4

VISIBILITÉ TOTALE

« Pour la première fois, nous savons à tout moment ce que voit un attaquant. »

« Visibilité totale » n'est pas un simple objectif ambitieux. C'est à cela que ressemble la gestion des risques de sécurité une fois tous les obstacles structurels des niveaux précédents levés : détection réactive, validation périodique, intervention manuelle et visibilité tardive de la direction. Le programme est continu, adaptatif et largement autonome. L'équipe de sécurité se concentre sur les décisions stratégiques et la gestion des exceptions, et non sur le tri des informations superflues ou la reconstruction manuelle des chemins d'attaque.

L'appellation ne ment pas. Pour la première fois, l'entreprise dispose d'une visibilité totale et en temps réel de sa surface d'attaque externe, telle que la voit un attaquant : non seulement les actifs existants, mais aussi ceux qui sont accessibles, ceux qui sont exploitables, la manière dont ils s'articulent entre eux, et à quoi ressemblent les chemins d'intrusion probables à l'instant précis. Cette vue d'ensemble est actualisée en continu à mesure que l'environnement évolue. Elle n'attend pas le prochain cycle d'analyse ou le prochain test d'intrusion.

Ce qui distingue le niveau « Visibilité totale », ce n'est pas une fonctionnalité en particulier, c'est la suppression des obstacles structurels qui caractérisent tous les autres niveaux. Il n'y a pas de période sans visibilité. Il n'y a pas de retard dans le tri dû à des vulnérabilités non validées. Il n'y a pas de décalage entre ce que le programme sait et ce que voit la direction. L'entreprise ne se contente plus de réagir aux failles, elle les anticipe.

Ce qui a permis d'en arriver là

L'entreprise a remplacé l'orchestration manuelle des scénarios d'attaque par une émulation automatisée qui s'adapte en permanence aux changements de l'environnement. Elle a comblé l'écart qui existait entre les données opérationnelles en temps réel et les rapports destinés à la direction. Et une décision de gouvernance a été prise : la mise en place de protocoles de réaction rapide pré-autorisés et de procédures d'escalade bien définies pour un fonctionnement autonome, ce qui a permis au programme de réagir à la vitesse de l'ordinateur sans intervention humaine à chaque étape.

The team is smaller relative to surface coverage than at any earlier stage — not because headcount was cut, but because automation has absorbed the work that previously required human triage. Expertise has concentrated upward. The security team works on problems that require judgement: threat modelling, adversarial scenario design, the strategic questions that cannot be automated. The CISO's relationship with the board has changed too. The conversation is no longer about what happened last quarter, it is about what the programme sees right now.

À quoi cela ressemble sur le plan opérationnel

Le discours de l'équipe de sécurité a évolué. La question n'est plus de savoir à quoi l'entreprise est exposée. Le programme y répond en permanence. Maintenant, il faut se demander à quelle vitesse il est possible d'y remédier et quelles sont les tâches les plus stratégiques sur lesquelles le personnel devrait se concentrer et que l'automatisation ne peut pas encore prendre en charge. Les rapports destinés au conseil d'administration sont directement créés à partir des données en temps réel du programme. Les équipes d'ingénierie reçoivent des rapports validés et transmis sans que le service de sécurité ait à les envoyer manuellement. Lorsqu'une nouvelle faille est découverte, le programme confirme en quelques heures, et non en plusieurs jours, si la surface est affectée.

À ce niveau, l'équipe de sécurité est plus restreinte proportionnellement à la surface couverte qu'aux niveaux précédents, car l'automatisation a absorbé la charge de travail qui nécessitait auparavant un tri manuel. Le niveau d'expertise s'est amélioré : l'équipe se concentre sur les problèmes qui nécessitent un esprit critique, et non sur ceux qui impliquent de traiter seulement du volume.

Ce qu'en disent les équipes

- « Nous détectons les nouvelles vulnérabilités avant même que les attaquants n'aient le temps de les exploiter. »
- « La question qui se pose désormais n'est pas de savoir si nous sommes exposés, mais à quelle vitesse nous pouvons remédier à cette exposition. »
- « Je peux présenter au conseil d'administration notre situation actuelle à partir des données générées au cours des dernières 24 heures. Cela n'était pas possible auparavant. »

Ce qu'il faut pour maintenir ce niveau

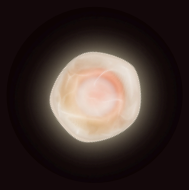
« Visibilité totale » n'est pas un objectif qui, une fois atteint, se maintient de lui-même. Les techniques d'attaque évoluent, et la qualité d'émulation du programme doit évoluer parallèlement. De nouvelles catégories d'infrastructures, notamment les systèmes d'IA, les flux de travail agentiques et les nouvelles intégrations SaaS, créent une surface d'attaque qui nécessite une mise à jour continue des modèles de détection et de validation.

Les exigences organisationnelles sont tout aussi importantes que les exigences techniques. Les structures de gouvernance doivent permettre un fonctionnement autonome sans y faire obstacle : cela implique des protocoles de réponse pré-autorisés, des seuils d'escalade clairement définis et un consensus au sein de la direction sur ce que signifie concrètement la « visibilité en temps réel de la posture de sécurité ». Les programmes qui atteignent le niveau « Visibilité totale » puis qui instaurent des barrières bureaucratiques autour de la réponse automatisée verront leurs capacités se dégrader pour revenir au niveau 3.

Le facteur le plus fréquent qui ramène au niveau 3 est un changement de direction : un nouveau RSSI qui réintroduit des étapes de contrôle manuel, ou un conseil d'administration qui perd confiance dans le fonctionnement autonome à la suite d'un faux positif. Maintenir le niveau « Vision totale » nécessite un entretien actif du mandat organisationnel, et pas seulement des capacités techniques.

Fonctionnalités qui caractérisent ce niveau

- Une émulation d'adversaire autonome qui s'adapte en continu aux changements de l'environnement sans intervention manuelle pour chaque scénario
- Une définition prédictive et dynamique des priorités qui s'adapte automatiquement à mesure que de nouvelles vulnérabilités apparaissent et que le contexte de la chaîne d'attaque évolue
- Un modèle de surface d'attaque en temps réel qui met en corrélation les changements liés à l'identité, à l'infrastructure, aux solutions SaaS et aux tiers pour former une image globale uniformisée et actualisée en continu
- Une intégration complète du programme, de la détection des vulnérabilités à la remédiation effective des problèmes, en passant par la validation des résultats, avec un minimum d'interventions manuelles



NIVEAU 1 → NIVEAU 2

Le passage du niveau 1 au niveau 2 peut se faire en quelques mois grâce à des efforts ciblés et à une responsabilité clairement définie.

NIVEAU 2 → NIVEAU 3

Le passage du niveau 2 au niveau 3 prend généralement entre six et dix-huit mois, en fonction de la complexité de l'environnement et du niveau d'intégration.

NIVEAU 3 → NIVEAU 4

La transition vers le niveau 4 est un processus continu ; elle nécessite un engagement opérationnel permanent et non une simple approche par projet. Ce qui accélère l'évolution, ce n'est pas la multiplication, mais la clarté : une responsabilité bien définie en matière d'exposition, une vision précise des objectifs à atteindre, et une mesure de la réduction effective du risque d'exploitation au lieu du simple suivi des tâches effectuées.

SECTION 4

OÙ VOUS SITUEZ-VOUS ?

La plupart des entreprises qui parcourent ces quatre niveaux constatent que leur situation réelle se situe entre deux niveaux. L'identification est plus mature que la validation. La validation est plus mature que la remédiation. Une note globale par niveau peut vous donner une idée approximative de votre situation. Elle ne permet toutefois pas de déterminer quelle dimension spécifique freine les autres.

Cette distinction est plus importante qu'il n'y paraît. Un programme dont la moyenne se situe au niveau 3 mais dont la validation correspond au niveau 1 n'est pas un programme de niveau 3. Il s'agit d'un programme présentant un obstacle opérationnel au niveau 1 qui freine les performances dans tous les autres domaines. Les SLA relatifs à la remédiation, les rapports destinés au conseil d'administration, le niveau d'automatisation : tout cela est limité par le maillon le plus faible, et n'est pas défini par le maillon le plus fort. La plupart des évaluations internes passent à côté de cette dimension, car elles notent la posture de sécurité globale au lieu de la décomposer par dimension opérationnelle.

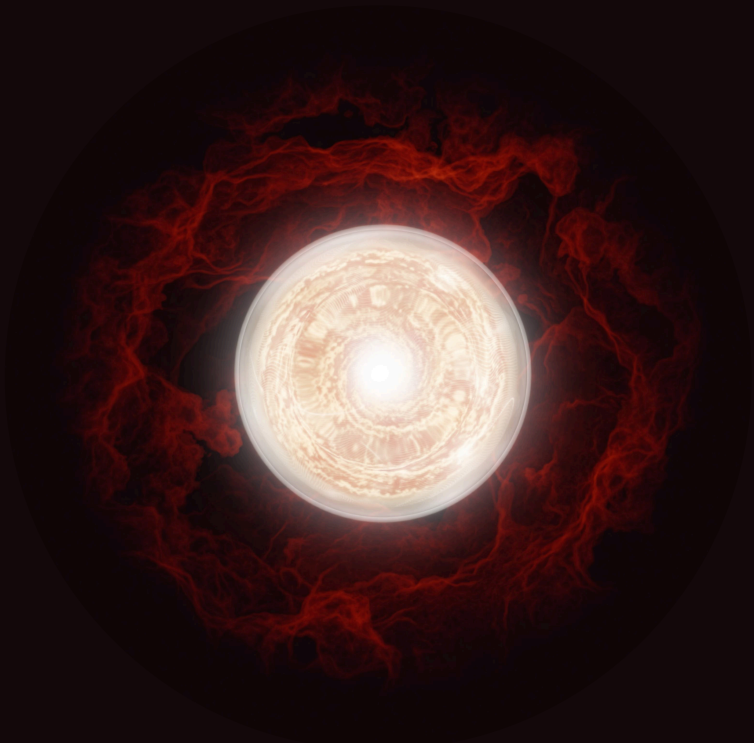
L'auto-évaluation interactive est conçue différemment. Elle évalue votre programme selon six critères distincts et les pondère afin d'identifier les domaines où l'écart entre votre situation réelle et votre profil de risque est le plus important. Le résultat n'est pas une donnée chiffrée, mais une analyse détaillée de votre situation par domaine, une mise en évidence de votre principal obstacle opérationnel et un plan d'action adapté à votre niveau, que votre équipe peut directement appliquer.

Même si vous connaissez déjà votre niveau global, il est utile de réaliser cette évaluation. C'est le profil détaillé par domaine qui apporte de la valeur dans les échanges avec la direction : l'enjeu n'est pas de dire « nous sommes au niveau 2 », mais plutôt « nous sommes au niveau 3 concernant l'identification et au niveau 1 concernant la validation, et voici le temps que l'on peut gagner dans la remédiation si nous comblons cet écart ».

ÉVALUEZ-VOUS :

Réalisez l’auto-évaluation interactive pour obtenir un profil de maturité personnalisé et un plan d’action

DÉCOUVREZ VOTRE NIVEAU DE MATURITÉ



Foire aux questions

Toutes les entreprises doivent-elles atteindre le niveau « Visibilité totale » ?

Non. Le niveau « Visibilité totale » s'adresse aux entreprises pour lesquelles les conséquences d'une intrusion justifient une validation continue et autonome. Pour de nombreuses entreprises, les niveaux 2 ou 3 conviennent à la majorité de leur surface d'attaque, les pratiques du niveau 4 étant réservées aux actifs les plus critiques. La bonne question n'est pas de savoir comment atteindre le niveau 4, mais quels actifs et quelles catégories de risques nécessitent un traitement de niveau 4.

Nous utilisons déjà de nombreux outils. Pourquoi notre niveau de maturité reste-t-il faible ?

L'intégration d'outils ne va pas de pair avec la maturité d'un programme. 93 % des entreprises utilisent des programmes de détection de vulnérabilité ; seuls 40 % ont adopté les tests d'intrusion automatisés. Pour la plupart des entreprises, l'intégration de multiples outils ne s'est pas traduite par une remédiation plus rapide des failles. En effet, le facteur limitant n'est pas le nombre d'outils en soi, mais leur capacité à s'insérer dans une structure qui valide l'exploitabilité, s'intègre à la remédiation et mesure les résultats réels plutôt que le simple volume d'activité.

Notre programme CTEM est actif. Pourquoi cela ne se traduit-il pas par une remédiation plus rapide ?

La plupart des programmes CTEM mesurent leur succès selon des critères qui ne reflètent pas la réduction réelle des risques. 67 % des entreprises évaluent la CTEM en fonction des lacunes de couverture identifiées ; seuls 33 % mesurent la réduction des vulnérabilités exploitables au fil du temps. Sans une validation de l'exploitabilité comme résultat prioritaire, et sans une attribution claire des responsabilités permettant d'associer les vulnérabilités validées aux personnes capables de les corriger, la CTEM génère davantage de vulnérabilités sans améliorer les résultats qui comptent.

Nous avons une visibilité totale sur le processus. Pourquoi notre exposition aux vulnérabilités ne diminue-t-elle pas ?

L'identification et la validation sont deux problématiques distinctes, mais la plupart des programmes les traitent comme un seul et même sujet. Élargir la couverture de l'EASM ou augmenter la fréquence des analyses génère davantage de résultats, mais en l'absence de mécanisme automatisé permettant de confirmer quels résultats sont réellement exploitables, cela se traduit par une accumulation des retards, et non par une amélioration de la posture de sécurité. Une identification accrue sans capacité de validation alourdit la charge de travail des analystes sans réduire les risques exploitables. La difficulté réside rarement dans le nombre de vulnérabilités identifiées par le programme, mais dans le nombre de ces résultats pouvant être confirmés comme réels et transmis pour remédiation avant qu'un attaquant passe à l'action.

About Hadrian

Hadrian is an offensive security platform designed for teams that need concrete data, not predictions. While traditional tools rely on a known inventory, Hadrian starts from a situation with no defined perimeter: the system identifies assets, maps attack paths, and verifies vulnerabilities as an attacker would, rather than as a conventional detection program would. It operates continuously, without scanning windows or testing cycles, so there is no gap between the actual state of your environment and what your program knows about it.

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

LOGOS DES CLIENTS

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

ET PLUS DE 300 AUTRES