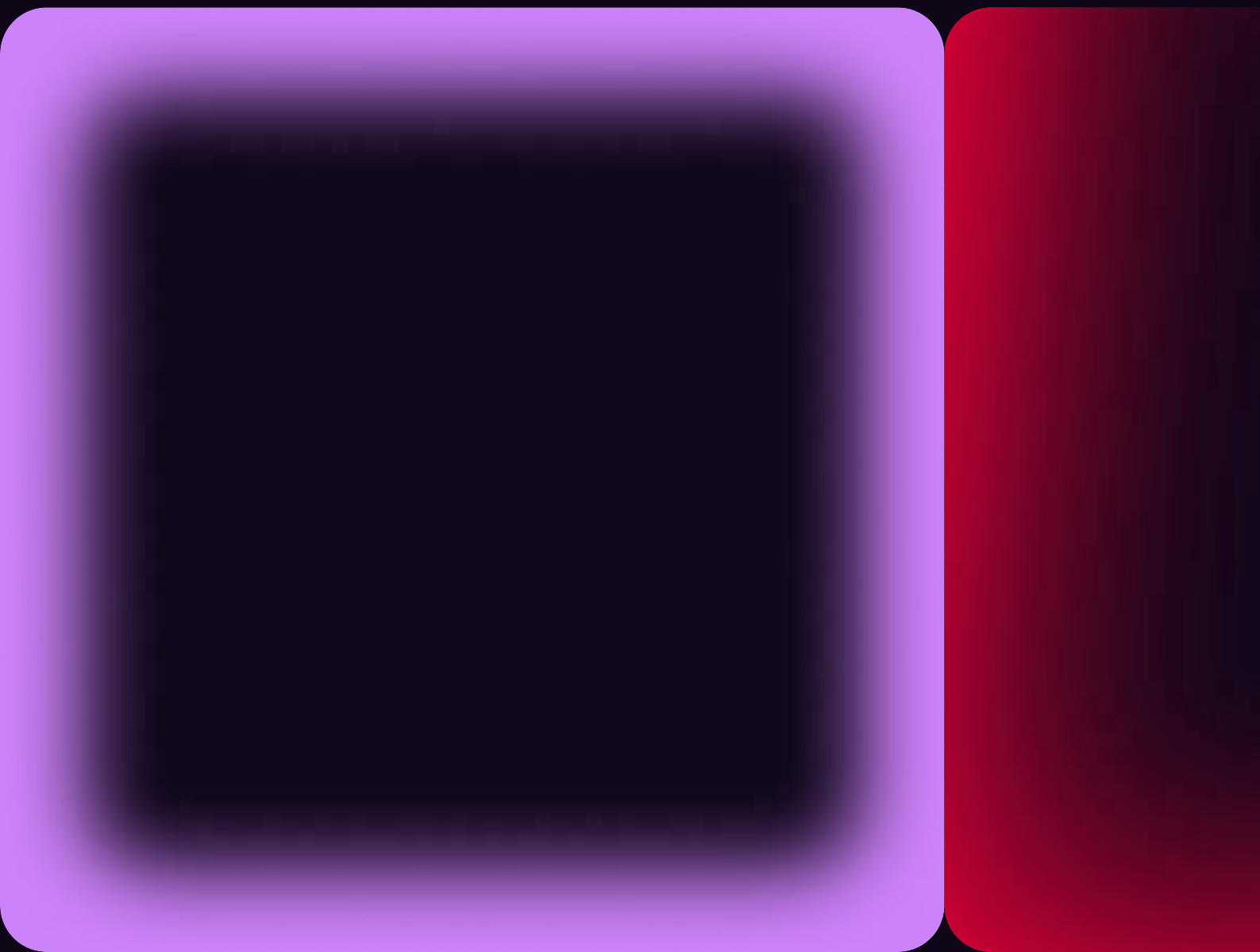
HADRIAN

WHITEPAPER

# L'avantage de la vitesse : comment adapter la stratégie de sécurité au rythme des pirates grâce à l'AEV



# Table des matières

# Résumé

En 2022, les pirates informatiques détectaient les vulnérabilités dans les 15 minutes qui suivaient leur découverte. Et c'était il y a trois ans, avant l'apparition des outils de piratage basés sur l'IA. L'IA est un facteur décisif dans cette accélération. Cette vitesse vertigineuse de l'émergence des attaques est en partie due aux menaces générées par l'IA, qui permettent aux pirates d'automatiser la reconnaissance, d'exploiter les vulnérabilités et d'étendre leurs opérations plus rapidement que les spécialistes de la défense ne sont capables de riposter.

Selon le Verizon 2025 Data Breach Incident Report, les violations causées par l'exploitation de vulnérabilités ont augmenté de 275 % au cours des deux dernières années — alimentées par les exploits zero-day et une identification plus rapide des dispositifs en périphérie. Parallèlement, le délai médian pour corriger une vulnérabilité exposée à Internet est de 32 jours, et près d'un tiers ne sont jamais corrigées. En 2025, CrowdStrike a signalé un temps moyen de breakout de seulement 48 minutes — avec un cas record en seulement 51 secondes. Face à des adversaires dopés à l'intelligence artificielle, la détection ne suffit plus — les organisations doivent désormais donner la priorité à la prévention.

C'est ici que **l'Adversarial Exposure Validation (AEV)** change la donne. En émulant en continu le comportement des attaquants depuis l'extérieur, l'AEV valide en temps réel quelles expositions sont réellement exploitables. Elle réduit la fatigue liée aux alertes, élimine les suppositions, et donne aux équipes de sécurité le pouvoir d'agir avant qu'un incident ne se produise — et non après.

**Les attaquants n'attendent pas. Vous ne pouvez pas non plus.**

# 1. La vitesse tue

Le secteur de la cybersécurité sait depuis longtemps que la rapidité est le facteur décisif pour prévenir et limiter les effets d'une atteinte à la sécurité. Mais le « temps du compromis » s'est réduit à un niveau que peu de gens avaient anticipé. Le temps de propagation (c'est-à-dire le temps qui s'écoule entre l'intrusion initiale d'un adversaire et son mouvement latéral au sein d'un réseau) ne se mesure plus en jours, en heures, voire en dizaines de minutes, désormais, il se mesure souvent en secondes.

Le rapport mondial sur les menaces de CrowdStrike en 2025 dresse un bilan très sombre de la situation. Sur des milliers d'analyses d'incidents, le temps moyen de propagation est de seulement 48 minutes. Il est alarmant de constater que certaines séries d'intrusion ont affiché des vitesses de propagation inférieures à une minute. Dans un cas très médiatisé attribué à un groupe organisé de cybercriminels à motivation financière, un mouvement latéral complet dans un environnement de cloud hybride s'est produit en l'espace de 51 secondes.

En 2022, les pirates informatiques détectaient les vulnérabilités dans les 15 minutes qui suivaient leur découverte. En 2022, nous en sommes aux balbutiements de l'IA générative. Trois ans après le début de cette nouvelle ère, les pirates informatiques ont su exploiter des outils d'IA pour rendre leurs opérations plus rapides, plus efficaces et plus dangereuses. Cette fenêtre de 15 minutes s'est probablement réduite à quelques secondes.

01 Cette rapidité crée des défis opérationnels majeurs pour les défenseurs.

02 Les modèles de langage à grande échelle sont désormais utilisés pour automatiser la découverte de vulnérabilités, enchaîner des failles de faible gravité pour créer de véritables exploits, et cibler des actifs exposés à une échelle et une vitesse jamais vues auparavant.

03 Cela montre bien que la défense, par nature, arrive déjà trop tard.

# Les référentiels historiques ne sont pas assez réactifs

Pour compliquer encore la tâche, les pratiques de gestion des correctifs restent terriblement lentes par rapport à la vitesse d'exploitation des acteurs de la menace. Le rapport DBIR 2025 de Verizon a révélé que le temps moyen pour remédier aux vulnérabilités des systèmes orientés vers l'Internet est de 32 jours. Par ailleurs, environ 30 % des vulnérabilités identifiées sur les appareils périphériques restent totalement sans correction. Étant donné que l'exploitation des nouvelles vulnérabilités identifiées commence souvent dans les 5 jours (voire le jour même de l'identification pour les dispositifs périphériques), il est évident que les stratégies de défense basées sur les correctifs sont insuffisantes pour lutter contre les cybercriminels modernes.

LES HACKERS SCANNENT LES VULNÉRABILITÉS QUELQUES MINUTES APRÈS LEUR DIVULGATION

**<15 MINUTES**

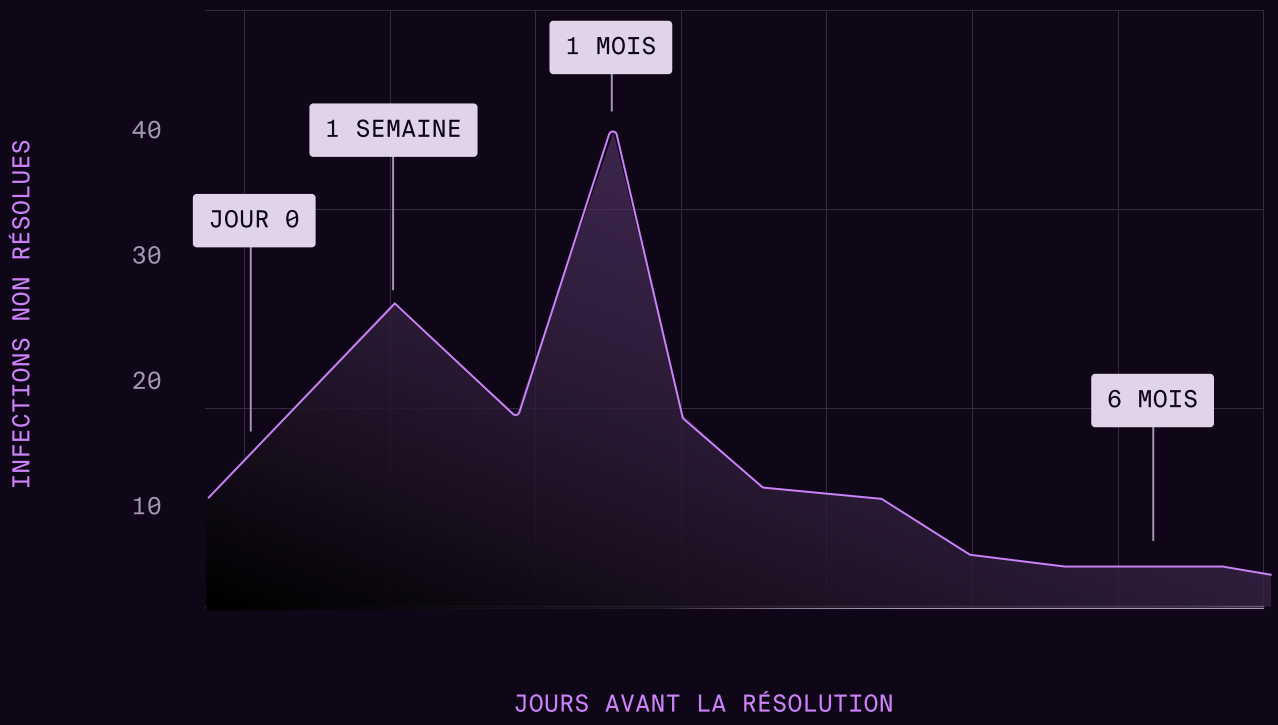
AUGMENTATION DE L'EXPLOITATION DES VULNÉRABILITÉS DEPUIS 2023

**+275%**

TEMPS MOYEN DE BREAKOUT EN 2025

**48 MINUTES**

TEMPS DE REMÉDIATION DES VULNÉRABILITÉS DANS LES SYSTÈMES EXPOSÉS À INTERNET



# La dette opérationnelle vous ralentit

La deuxième source de pression à laquelle sont confrontés les RSSI est le manque de ressources. Les RSSI gèrent plus d'outils que jamais, mais avec des effectifs stables, voire en baisse. Les budgets sont examinés à la loupe. Les équipes de sécurité croulent sous les alertes et sont obligées de trier les risques sans contexte. De nombreuses entreprises n'ont tout simplement pas le personnel nécessaire pour examiner tous les problèmes signalés, valider toutes les menaces ou trier les faux positifs. Ce ne sont là que quelques-unes des restrictions opérationnelles auxquelles sont confrontées les équipes SOC :

01 Une multitude d'outils de sécurité dont la maintenance mobilise du temps et des ressources au sein des équipes SOC.

02 Les équipes de sécurité développent une fatigue d'alerte et accumulent les tâches en attente.

03 Les rapports de conformité détournent l'attention des priorités opérationnelles.

La visibilité en silo est l'un des défis les plus redoutables auxquels sont confrontés les responsables de la sécurité. C'est tout ce que vous ne voyez pas qui donne aux pirates plus de munitions et d'occasions pour exploiter vos vulnérabilités.

Les fusions-acquisitions s'accompagnent souvent d'infrastructures héritées, de sous-domaines inconnus et d'anciens systèmes qui n'ont pas été conçus dans un souci d'uniformisation des contrôles de sécurité.

Parallèlement, les équipes marketing lancent régulièrement des microsites de campagne, enregistrent de nouveaux domaines ou utilisent des outils tiers sans contrôle de la sécurité. Ces activités peuvent collecter des données sensibles ou s'intégrer dans des systèmes internes, mais elles sont rarement suivies par les services informatiques ou couvertes par les procédures de gestion des vulnérabilités.

Finalement, ces silos fragmentent la visibilité et créent des lacunes que les pirates exploitent avec une rapidité à laquelle il est impossible de répondre. L'informatique de l'ombre prospère dans ces angles morts, créant des risques que l'équipe de sécurité n'identifie que trop tard. Une fois encore, la sécurité préventive est la seule méthode pour avoir une visibilité continue sur la surface d'attaque.

## La défense statique présente des inconvénients

Dans ce contexte, les autres modèles de sécurité (basés sur l'analyse ponctuelle, les listes de vérification de conformité et les tests de pénétration annuels) ne sont pas adaptés aux attaques qui évoluent à un tel rythme. La validation manuelle des correctifs ne peut espérer rivaliser avec des pirates opérant à la vitesse de l'IA. Même s'ils sont précieux, les exercices trimestriels de la Red Team n'apportent une garantie que sur le moment où ils sont réalisés et uniquement dans le périmètre qui leur est assigné.

Dans un environnement où chaque seconde compte, les spécialistes de la défense ont besoin d'une visibilité, d'une validation et d'une hiérarchisation continues.

# Les indicateurs qui comptent

Face à des temps de propagation de 48 minutes, les performances en matière de sécurité doivent être mesurées avec de nouveaux indicateurs clés de performance (KPI) :

- **Mean Time to Prevent (MTTP):** rapidité avec laquelle les risques peuvent être identifiés, validés et corrigés en cas de faille exploitable.
- **Mean Time to Validate (MTTV):** rapidité avec laquelle les risques sont confirmés comme étant exploitables.
- **Mean Time to Remediate (MTTR):** rapidité avec laquelle les failles critiques sont corrigées ou neutralisées.

Les entreprises qui ne se fixent pas d'objectifs ambitieux pour ces paramètres ne sont plus seulement des « retardataires » en matière de bonnes pratiques, elles sont fondamentalement en danger.

En 2025 et dans les années à venir, les opérations de sécurité devront être menées avec la conviction que chaque minute compte. Qu'il s'agisse de réseaux de ransomware, de groupes APT ou de pirates opportunistes, la capacité à valider et à hiérarchiser rapidement les risques réels définira de plus en plus les gagnants et les perdants.

# 2. D'autres outils peuvent vous mener loin, mais jusqu'à un certain point

La nature de la cybersécurité est telle que de nombreux outils sont souvent utilisés pour garder une longueur d'avance sur toutes les cybermenaces. Mais tous ces outils ne se valent pas.

Les outils ponctuels, les tests de pénétration périodiques et les inventaires d'actifs témoignent d'un modèle de sécurité réactif. S'ils sont encore utiles dans certains contextes, ces outils sont désormais obsolètes dans un monde défini par des menaces en temps réel et des surfaces d'attaque externes qui changent d'heure en heure.

# Les alertes qui crient au loup

Un grand nombre d'alertes entraîne rapidement ce qu'on appelle la fatigue d'alerte. Les équipes de sécurité croulent sous les rapports sur les vulnérabilités et sous les inventaires d'actifs qui ne sont pas classés par ordre de priorité. Sans validation, les équipes perdent un temps précieux à trier des expositions qui sont en réalité des faux positifs ou des risques minimes. Dans le même temps, des vecteurs véritablement exploitables peuvent être noyés dans la masse ou ne pas être pris en compte du tout. Voici quelques exemples d'alertes qui génèrent beaucoup de bruit :

CVE DE FAIBLE GRAVITÉ :

Alertes concernant des bibliothèques obsolètes ou des vulnérabilités mineures qui ne présentent qu'un risque limité dans le monde réel, en particulier lorsqu'il n'y a pas de faille d'exploitation viable ou qu'elles sont protégées par des contrôles compensatoires.

ACTIFS INTERNES UNIQUEMENT :

Constatations sur les systèmes non exposés à l'Internet public (comme des environnements de développement ou des services en arrière-plan) qui sont signalés alors qu'ils sont inaccessibles aux attaquants externes.

# Bienvenue dans la « comédie sécuritaire »

Les tests de pénétration périodiques ne sont pas une solution suffisante. Même les meilleurs tests de pénétration manuels sont généralement programmés tous les trimestres ou tous les ans. Cela entraîne une forme de « comédie sécuritaire » : vous vous sentez protégé parce que vous avez effectué un test le mois dernier, mais votre surface d'attaque a évolué depuis.

Les inventaires d'actifs statiques aggravent le problème. Dans les environnements hybrides et cloud natif, la multiplication des actifs n'est pas seulement courante, elle est la norme. S'appuyer sur des listes établies manuellement, c'est définir votre stratégie de sécurité sur une image incomplète - et pire encore, cela signifie que vous ne testez probablement qu'une petite partie de cette image. Les alertes les plus dangereuses sont souvent celles que vous ne recevez jamais, simplement parce que l'actif est resté inconnu ou n'a pas été inclus dans le champ d'application au départ.

En outre, aucune de ces méthodes ne reproduit les adversaires du monde réel. Elles ne reproduisent pas les TTP (Tactiques, Techniques et Procédures) de bases de connaissance telles que MITRE ATT&CK. Elles n'évaluent pas l'efficacité de vos capacités de détection et de réaction. Elles ne tiennent pas compte de la capacité du pirate à combiner plusieurs failles en un seul scénario dévastateur.

Les responsables de la sécurité le savent bien. Les RSSI sont parfaitement conscients que leurs équipes sont surchargées de travail, manquent de ressources et sont toujours dans la gestion des urgences. Ils savent que la question n'est pas de savoir s'il y a des risques, car toutes les entreprises en ont, mais de savoir si ces risques sont exploitables et s'ils peuvent être évités avant que les cybercriminels n'agissent.

C'est là que la validation de l'exposition aux menaces commence à combler cette lacune. Mais avant de se concentrer sur son fonctionnement, voyons de quoi il s'agit vraiment.

# 3. La pièce manquante : la validation de l'exposition aux menaces (AEV)

La validation de l'exposition aux menaces (AEV) est un nouveau paradigme en matière de validation de la sécurité, qui intègre la logique du pirate dans la gestion quotidienne de l'exposition. Il ne s'agit pas simplement d'une méthode de test, mais d'une capacité opérationnelle conçue pour simuler le comportement d'un adversaire de manière continue et précise.

Fondamentalement, l'AEV consiste à reproduire en permanence l'activité des attaquants externes afin d'identifier les vulnérabilités réellement exploitables. Dans un monde où les menaces générées par l'IA automatisent la reconnaissance et la diffusion des failles, l'AEV répond à une question plus urgente : *quel est l'état général de ma vulnérabilité ?*

# Se mettre à la place de l'adversaire

**L'AEV opère de l'extérieur vers l'intérieur. Elle considère votre environnement de la même manière qu'un pirate le ferait, c'est-à-dire d'un point de vue externe et sans autorisation.** Ce facteur est essentiel, car il élimine l'hypothèse selon laquelle la visibilité interne est synonyme de sécurité. De nombreuses entreprises disposent d'inventaires et de politiques de correctifs bien documentés, mais cela ne signifie pas que leur périmètre est sécurisé. L'AEV identifie les actifs inconnus, non gérés ou mal configurés que d'autres outils peuvent ignorer.

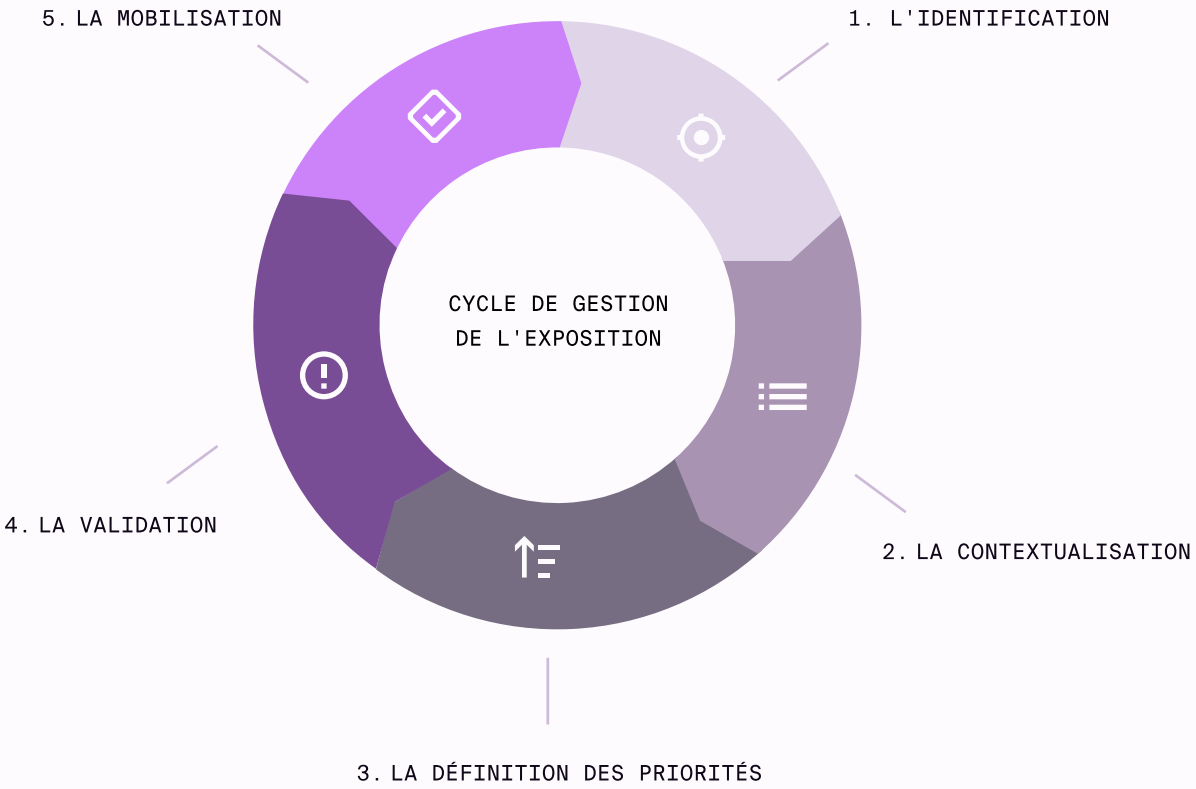
L'AEV se distingue du travail de la Red Team, des outils BAS (Breach and Attack Simulation) et d'autres évaluations de vulnérabilité. Contrairement aux Red Teams, l'AEV fonctionne en continu et de manière autonome. Contrairement aux outils BAS, qui reproduisent souvent des chaînes d'attaques prédéfinies dans un environnement de type laboratoire, l'AEV cible votre périmètre réel. Cette méthode ne s'arrête pas à l'identification d'une CVE, elle détermine aussi si la faille est accessible, si elle est exploitable et si elle présente un risque important pour l'entreprise.

Elle complète parfaitement la gestion des surfaces d'attaque externes (EASM). L'EASM se concentre sur l'identification et l'inventaire des actifs connectés à Internet. L'AEV prolonge l'EASM en demandant : et après ? Elle passe au crible l'inventaire et identifie les actifs qui représentent de véritables menaces, en particulier ceux qui pourraient être exploités rapidement par des tactiques automatisées ou renforcées par l'IA.

# La philosophie unitaire de la CTEM

La puissance opérationnelle de l'AEV réside dans son intégration dans des cadres plus larges de gestion continue de l'exposition aux menaces (CTEM). La CTEM est une approche structurée de la réduction de l'exposition qui se concentre sur l'identification, l'évaluation, l'ordonnancement, la validation et la correction des risques, avant qu'ils ne deviennent exploitables. Elle adapte les pratiques de sécurité à la rapidité et à la fluidité des menaces modernes, en particulier celles induites par l'automatisation de l'IA.

**La CTEM comprend cinq phases clés :**




**L'AEV intervient dans les phases de définition des priorités et de validation.** Elle apporte des preuves concrètes qui permettent d'établir des priorités et de mettre en place des flux de travail correctifs intelligents et ciblés. Elle complète l'identification et la contextualisation de l'EASM et permet aux équipes de sécurité de se concentrer sur la correction.

Les simulations de l'AEV sont conçues pour s'arrêter à l'accès initial. C'est essentiel pour la sécurité et la conformité. L'objectif n'est pas de pénétrer dans le réseau ou d'extraire des données, mais de déterminer si l'accès a été possible. Ce choix de conception permet à l'AEV de fonctionner en toute sécurité dans des environnements de production, sans perturber les opérations ou violer les limites de la vie privée.

D'un point de vue technologique, les plateformes AEV utilisent généralement l'automatisation orchestrée, en s'appuyant sur des moteurs d'analyse, des structures de simulation de failles et d'imitation des comportements. Elles peuvent aussi être enrichies avec des renseignements sur les menaces afin d'imiter les dernières TTP observées sur le terrain. Les plateformes les plus avancées intègrent une logique pilotée par l'IA pour hiérarchiser les cibles en fonction de leur exploitabilité et de leur niveau de risque pour l'entreprise.

Pour les RSSI et les responsables de la sécurité, la valeur de l'AEV réside dans sa précision et son efficacité. En validant les failles en continu, l'AEV ne fait apparaître que les résultats pertinents. Cela réduit la fatigue d'alerte, affine les flux de travail correctifs et permet aux équipes de sécurité de se concentrer sur les résultats stratégiques plutôt que sur les bruits tactiques.

Pour résumer, l'AEV ne se contente pas de vous signaler où vous pourriez être vulnérable, elle vous montre ce que les pirates peuvent exploiter dès maintenant.

# 4. Pourquoi l'AEV redéfinit la vitesse

L'un des aspects les plus convaincants de la validation de l'exposition aux menaces réside dans sa rapidité inhérente. Non seulement en termes de rapidité d'identification des menaces, mais aussi de rapidité de réaction. Dans un environnement de menaces où les pirates peuvent se déplacer latéralement en quelques minutes, la vitesse n'est pas un luxe, c'est une condition sine qua non.

Les plateformes AEV sont conçues pour fonctionner en continu. Contrairement aux analyses périodiques ou aux tests programmés, l'AEV fonctionne en temps réel, validant les expositions au fur et à mesure qu'elles surviennent. Cela signifie que dès qu'un actif mal configuré est exposé à Internet ou qu'une nouvelle CVE devient pertinente pour votre périmètre, l'AEV peut détecter et simuler son exploitation en quelques minutes.

# Fermer la « fenêtre de risque »

Cette rapidité est essentielle. Envisagez une autre solution : une analyse est lancée chaque semaine et, pendant ce temps, un pirate a identifié la même vulnérabilité et est passé de l'accès initial à la violation complète du domaine. Le délai entre l'identification et l'action (que l'on peut appeler la « fenêtre de risque ») doit être réduit au minimum, et l'AEV est spécialement conçu pour cela.

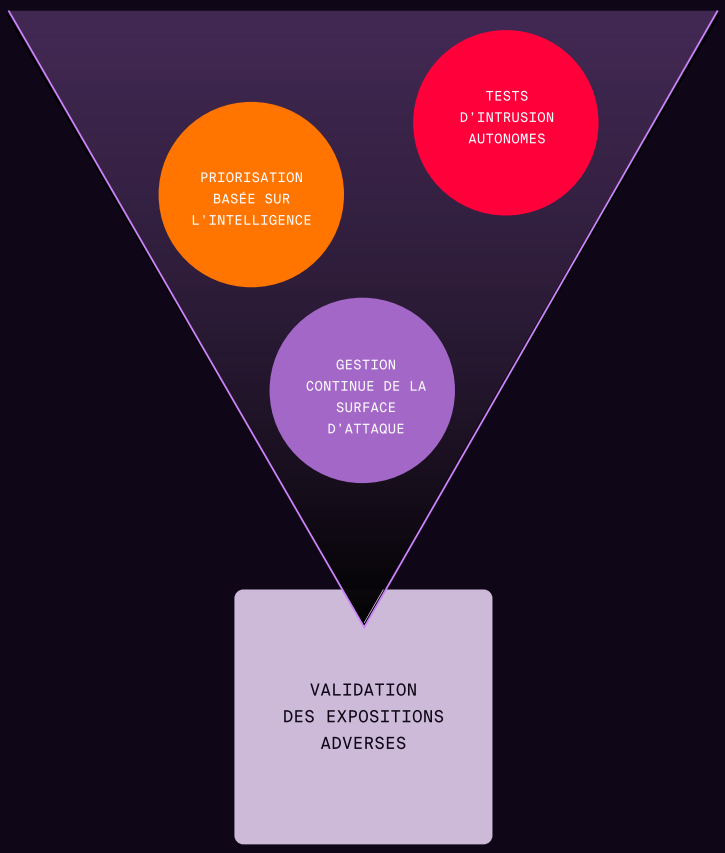
La rapidité de l'AEV tient en partie à sa conception architecturale. Les plateformes modernes de validation de l'exposition aux menaces sont généralement fournies via SaaS, ce qui permet des évaluations évolutives et à la demande sans les frais généraux d'un déploiement sur site. Selon Gartner, les solutions de pointe s'appuient souvent sur l'automatisation et l'infrastructure cloud natif pour reproduire le comportement d'un pirate sur des actifs externes avec un minimum de perturbations.

L'automatisation permet également de gagner en rapidité. Les plateformes AEV comme celle d'Hadrian utilisent des moteurs d'orchestration pour déterminer les expositions aux menaces à tester, la manière de les tester et les mesures à prendre en fonction des résultats. Il n'est donc plus nécessaire d'intervenir manuellement à chaque étape, ce qui accélère considérablement le processus de validation.

L'AEV élimine surtout les délais liés au tri. D'autres programmes de détection accumulent des milliers de résultats dans une file d'attente qui doit être examinée manuellement et classée par ordre de priorité. L'AEV fournit des **résultats validés, basés sur des exploits.** Il ne s'agit pas de risques théoriques, mais de menaces avérées et classées par ordre de priorité. Ainsi, les équipes de sécurité ne perdent pas de temps à débattre de la gravité ; elles peuvent passer directement à la remédiation.

# Élément d'un flux de travail équilibré en matière de sécurité

L'AEV s'intègre également parfaitement aux flux de travail existants. Les failles validées peuvent être transmises directement aux plateformes SIEM et SOAR, ou aux systèmes de gestion de tickets comme Jira, pour une action immédiate. Enfin, la rapidité de l'AEV permet d'obtenir des résultats plus stratégiques en matière de sécurité. Une validation rapide entraîne une remédiation plus rapide, ce qui permet de resserrer les boucles de rétroaction. Au fil du temps, les entreprises qui utilisent l'AEV constatent une amélioration de leur maturité opérationnelle. Elles réduisent leur MTTR moyen, commettent moins d'erreurs sous la pression et commencent à anticiper le comportement des pirates au lieu de simplement y faire face.



# 5. Scénarios de rapidité dans le monde réel

Les RSSI qui cherchent à justifier leur investissement dans la validation de l'exposition aux menaces (AEV) doivent comprendre comment cette approche permet de mettre en place des mesures préventives dans un scénario concret. Ce qui suit est un aperçu de la façon dont l'AEV fonctionne dans des scénarios de menace critique et urgente, mettant en évidence sa rapidité et sa précision par rapport à d'autres outils de sécurité.

# Scénario : une interface d'administration mal configurée exposée

Une entreprise lance une nouvelle application SaaS en utilisant l'infrastructure en tant que code. Dans la précipitation pour respecter le délai de publication, un environnement de développement (avec un panneau de connexion administrateur) est accidentellement laissé accessible au public sur Internet. Au sein de l'entreprise, personne n'a conscience de l'exposition.

Un programme de détection pourrait repérer cet élément lors de la prochaine analyse programmée, plusieurs jours, voire plusieurs semaines après. Pendant ce temps, l'actif exposé peut être identifié par quiconque effectue des analyses à grande échelle à l'aide d'outils tels que Nmap.

Avec l'AEV mise en place, la mauvaise configuration est détectée en quelques minutes. Le système AEV reproduit un pirate ciblant l'espace IP, localise l'interface d'administration, confirme qu'elle est accessible et qu'elle manque de contrôles de base, et valide immédiatement l'exposition comme étant exploitable. Comme le système est conscient du contexte commercial (cette application communique avec une base de données contenant des dossiers de clients), il signale le problème comme hautement prioritaire.

Une alerte est générée et envoyée à l'ingénieur en sécurité approprié avec des conseils complets de remédiation. Tout cela se fait en temps réel et ne laisse aucune chance à vos adversaires d'exploiter la vulnérabilité.

TEMPS ÉCOULÉ ENTRE L'EXPOSITION ET LA VALIDATION

12 MINUTES

DÉLAI DE RÉSOLUTION PRÉVENTIVE

<90 MINUTES

# Scenario: nouveau cas zero day

Une vulnérabilité de type « zero day » affectant une application de serveur web très répandue a été révélée et un code POC publié. En l'espace de quelques heures, des tentatives d'exploitation se multiplient sur Internet.

Certaines équipes de sécurité se démènent, souvent manuellement, pour recouper cette nouvelle CVE avec les inventaires d'actifs.

Avec l'AEV, dès que la CVE est révélée, la plateforme analyse tous les actifs externes connus et reproduit le chemin d'exploitation contre eux. Sur les 50 serveurs utilisant la version vulnérable, 3 sont confirmés comme étant accessibles depuis l'extérieur et sans correctif. L'exposition est validée en temps réel et des tâches sont générées automatiquement pour l'équipe chargée des opérations informatiques.

Ce processus permet non seulement de gagner du temps, mais aussi d'éviter les angles morts. **Cela permet de passer d'une réponse désordonnée à l'échelle de l'entreprise à un plan d'action préventif et ultra ciblé.**

# 6. Former une équipe de spécialiste qui réagit rapidement avec l'AEV

L'adoption de l'AEV n'est pas seulement une décision qui concerne un outil, c'est un changement de modèle opérationnel. Cette section explique comment mettre en place un programme qui utilise l'AEV pour réduire les fenêtres de risque et améliorer la gestion de l'exposition.

# Trois conditions de déclenchement du test avec l'AEV

Les systèmes AEV sont plus efficaces lorsqu'ils sont directement associés à des événements d'exposition. La plateforme Hadrian, par exemple, déclenche une validation automatique en réponse aux éléments suivants :

01 **Exposition d'un nouvel actif -** Toute nouvelle adresse IP, tout nouveau service ou domaine accessible depuis l'extérieur.

02 **Modifications des actifs existants -** Modifications des configurations, des listes de contrôle d'accès (ACL) ou des systèmes de noms de domaine (DNS) qui modifient le niveau de risque.

03 **Émergence de nouveaux exploits ou de nouvelles techniques, tactiques et procédures (TTP) -** Qu'ils proviennent de flux d'informations sur les menaces ou qu'ils aient été découverts grâce à la surveillance du dark web.

Ce modèle basé sur les événements garantit que l'AEV ne fonctionne pas seulement sur la base du temps, mais aussi en fonction du contexte.

# Des indicateurs opérationnels qui comptent

Nous avons déjà mentionné ces statistiques, mais répétons-les. Pour évaluer l'impact de l'AEV, les responsables de la sécurité doivent contrôler les éléments suivants :

- **MTTP (Mean Time to Prevent):** rapidité avec laquelle les risques peuvent être identifiés, validés et corrigés en cas de faille exploitable.
- **MTTV (Mean Time to Validate):** temps nécessaire pour déterminer si l'exposition est réellement exploitable.
- **MTTR (Mean Time to Remediate):** temps écoulé entre la validation et la résolution ou l'atténuation.

L'AEV réduit considérablement le MTTV (de plusieurs jours à quelques minutes) et en fournissant des données claires et validées, elle accélère également le MTTR. L'addition de ces deux indicateurs et du MTTD donne le MTTP. Lorsque les résultats ne sont pas hypothétiques, il y a moins de résistance de la part des services informatiques et une exécution plus rapide de la part des équipes de développement et d'exploitation.

# Stratégies de remédiation basées sur les rôles

L'intérêt de l'AEV est multiplié lorsqu'elle est associée à un système de responsabilité plus large. Mais elle peut être tout aussi efficace pour les équipes plus réduites, car elle automatise une grande partie du processus.

Les résultats de l'AEV sont également pris en compte dans les registres de risques, les rapports pour le conseil d'administration et les tests de contrôle continus, ce qui permet de relier l'approche de sécurité à la supervision stratégique.

# 7. Correction rapide

Étant donné que les pirates testent les vulnérabilités dans les 15 minutes (voire plus rapidement s'ils utilisent des outils d'IA) qui suivent leur découverte, vous n'avez littéralement pas une seconde à perdre. La seule façon de lutter contre la rapidité des attaques est d'améliorer la vitesse de prévention.

Contrairement à d'autres outils qui peuvent submerger les équipes de données, l'AEV apporte de la clarté. Contrairement aux Red Teams qui ne valident qu'occasionnellement et dans un certain périmètre, l'AEV valide en continu. Et contrairement aux modèles de risque qui sont spéculatifs, l'AEV prouve l'exploitabilité dans le monde réel.

Pour le RSSI et les équipes SOC, cela signifie un meilleur contrôle, une meilleure hiérarchisation des priorités et une réduction sensible du risque opérationnel. L'AEV réduit les délais, adapte les résultats techniques à l'impact commercial et permet à votre équipe de passer d'une gestion réactive à une résilience proactive en temps réel.

> Vous ne pouvez pas freiner les cybercriminels. Mais avec l'AEV, vous pouvez garder une longueur d'avance.