

B|ACKNOISE

EFFICACITÉ DE LA SÉCURITÉ OPÉRATIONNELLE

DEEP PURPLE REPORT 2026

v2.0 – māj août 2026

Edité par ERIUM

contact@erium.fr

erium.fr/blacknoise-aev/

INTRODUCTION

Pour la quatrième année consécutive, BlackNoise publie son rapport annuel sur l'efficacité de la sécurité opérationnelle.

Cette édition analyse plus de 2 000 simulations d'attaques exécutées en 2025 et au premier semestre 2026 sur des infrastructures de production. Elle intègre aussi les évolutions réglementaires et de l'état de la menace jusqu'en août. Les campagnes du premier semestre 2026 confirment les tendances observées sans les infléchir.

La tendance majeure de 2026 tient en une phrase :

La croissance du volume de vulnérabilités publiées, accélérée par des capacités offensives assistées par IA, rend la correction exhaustive hors d'atteinte.

À côté du « Patch First », un principe complémentaire s'impose, le « Response First » : plutôt que d'attendre une remédiation généralisée, garantir que les failles les plus exploitables déclenchent une réaction rapide, automatisée et proportionnée. Cette réaction se met en œuvre en quelques jours, là où un cycle de correctifs complet s'étale sur plusieurs mois. Mais une capacité de réaction ne se décrète pas, elle se vérifie : l'AEV est l'outil qui permet de tester cette chaîne en conditions réelles, de mesurer le délai entre l'exécution de l'attaque et l'action de blocage, et d'opérer le principe dans le temps à mesure que les configurations et les menaces évoluent.

Ce rapport s'adresse aux CISO et CIO qui souhaitent situer leur trajectoire par rapport à celle de leurs pairs et calibrer leurs investissements défensifs sur des données de terrain.



Pierre TEXIER / CTO
pierre.texier@erium.fr



Arnaud LE MEN / CEO
arnaud.lemen@erium.fr

A PROPOS DE BLACKNOISE AEV

Développée par la société Erium, BlackNoise est une plateforme d'Adversarial Exposure Validation (AEV) entièrement agentless, exploitable en modèle SaaS comme On-premise.

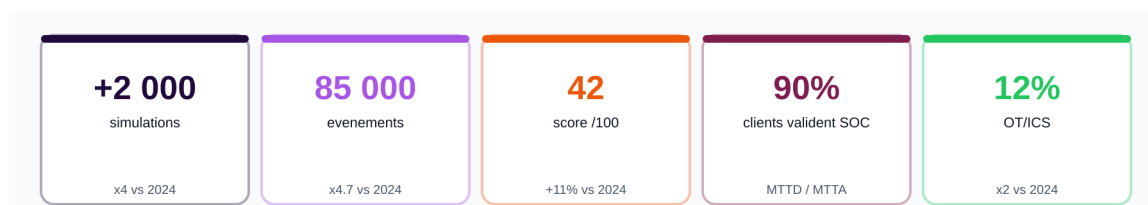
Conçue et développée par des experts de la sécurité opérationnelle, elle est utilisée par des organisations publiques et privées pour valider en conditions réelles l'efficacité opérationnelle de leurs investissements cyber.

BlackNoise combine la cartographie de la surface d'attaque (ASM), les tests automatisés de compromission (Automated Pentest) et un moteur avancé d'exécution des modes opératoires d'attaque (BAS). Cette convergence permet de répondre à plusieurs cas d'usage : la validation des capacités de détection et de réaction, la démonstration de conformité (DORA, NIS2, TIBER-EU) et l'entraînement des équipes cyber en charge de la gestion des incidents et des crises.



SYNTHÈSE — À RETENIR EN DEUX MINUTES

Ce que révèlent plus de 2 000 simulations d'attaques exécutées sur des environnements de production.



Chiffres clés de l'exercice 2025, BlackNoise AEV

Quatre constats

- **La détection progresse** (42/100, +11 % vs 2024) mais l'élargissement au cloud, à l'OT/ICS et à la *supply chain* déplace les angles morts.
- **Discovery, Exfiltration et Lateral Movement** restent les zones les plus fragiles, notamment face aux techniques Living-off-the-Land.
- **La validation de la réponse s'installe** : les organisations chronomètrent le MTTR et testent les contre-mesures automatiques avant activation.
- **La fréquence des simulations explique la progression** bien mieux que l'évolution des modèles de SOC interne, MSSP ou hybride.

La priorité

Passer du contrôle périodique à la capacité démontrée. L'AEV devient la couche de validation continue entre vulnérabilités ouvertes, outils de défense, pentest expert, gestion de crise, conformité et entraînement des équipes.

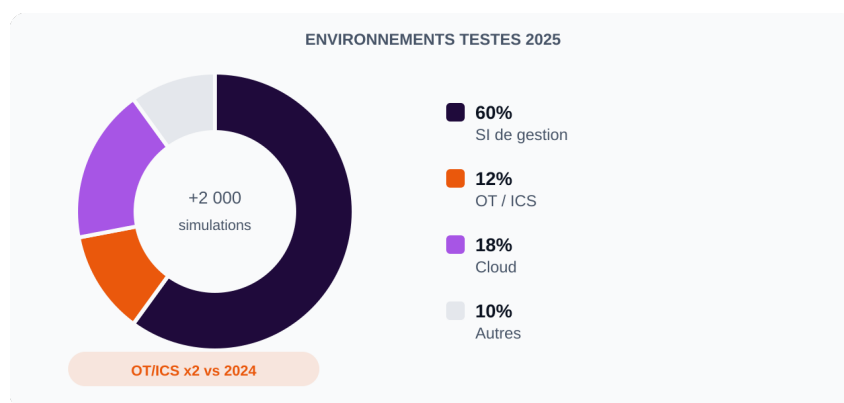
Les **cinq recommandations pour 2026/2027** figurent en fin de rapport.

1. CONTEXTE ET MÉTHODOLOGIE

Le **Deep Purple Report** synthétise les résultats techniques des simulations exécutées par la solution AEV de BlackNoise au cours de l'exercice 2025 et du premier semestre 2026. Tous les tests sont référencés selon le modèle ATT&CK du MITRE et donnent lieu à un score d'efficacité basé sur MTDD (Mean Time To Detect), MTTA (Mean Time To Acknowledge) et MTTR (Mean Time To React). Les séries d'évolution pluriannuelle s'arrêtent à 2025, dernier exercice complet, afin de préserver la comparabilité d'une année sur l'autre ; les campagnes du premier semestre 2026 alimentent les constats qualitatifs et les analyses de tendance.

1.1 Périmètre des organisations testées

Les simulations réalisées ont ciblé des infrastructures d'ETI et de grands groupes, tous secteurs confondus : public, finance et assurance, industrie, télécommunications, aéronautique, transport, distribution, santé.



Répartition des environnements testés en 2025

Les environnements industriels OT/ICS doublent leur part ($\times 2$ vs 2024), portés par la disponibilité croissante d'outils de détection dédiés. Le cloud accélère fortement, avec une première couverture structurée des environnements SaaS.

1.2 Notes méthodologiques

- Les résultats reflètent les organisations et périmètres testés par BlackNoise. Ils ne constituent pas un échantillon statistiquement représentatif du marché.
- Les indicateurs MTDD, MTTA et MTTR sont calculés selon les conventions BlackNoise et la disponibilité des journaux, alertes et retours opérateurs.
- Les cas d'usage décrivent des pratiques observées ou recommandées. Ils ne constituent ni une garantie de conformité réglementaire, ni une promesse d'économie ou de performance financière.

2. RÉSULTATS : ÉVALUATION DES CAPACITÉS DE DÉFENSE

2.1 Score global de détection

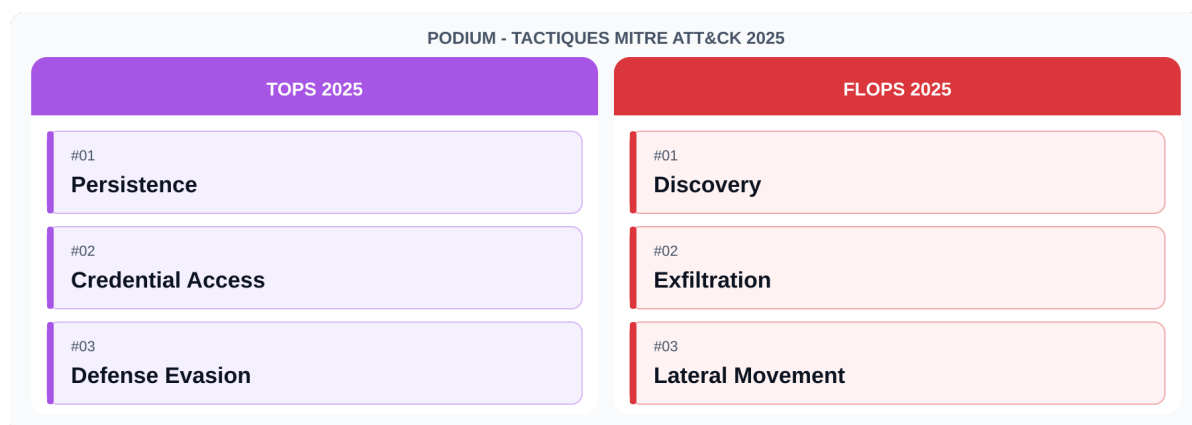
Les capacités de détection progressent pour la quatrième année consécutive. Le rythme se stabilise : signe de maturité sur les périmètres établis, et d'élargissement vers de nouveaux terrains.



Score moyen de détection, évolution 2022 à 2025

Le score de 42/100 en 2025 (+11 % vs 2024) traduit deux réalités. Les organisations les plus avancées approchent d'un palier sur les périmètres maîtrisés. L'élargissement vers l'OT/ICS, le cloud et la *supply chain* introduit de nouveaux angles morts qui pèsent sur le score global. L'écart entre organisations qui s'entraînent régulièrement et celles qui démarrent reste significatif : la régularité est le premier facteur de progression, indépendamment du modèle SOC.

2.2 Podium tops et flops



Tops et flops de détection par tactique MITRE ATT&CK, 2025

La Persistence monte en première position des tops : les mécanismes de détection se sont affinés sur les techniques de maintien d'accès. Discovery reste en tête des flops pour la troisième année consécutive, l'empreinte des techniques LotL (Living-off-the-Land) en demeurant la principale cause. L'Exfiltration remonte dans les flops : la diversification vers des protocoles alternatifs et des services cloud standards complexifie la distinction entre trafic légitime et exfiltration malveillante.

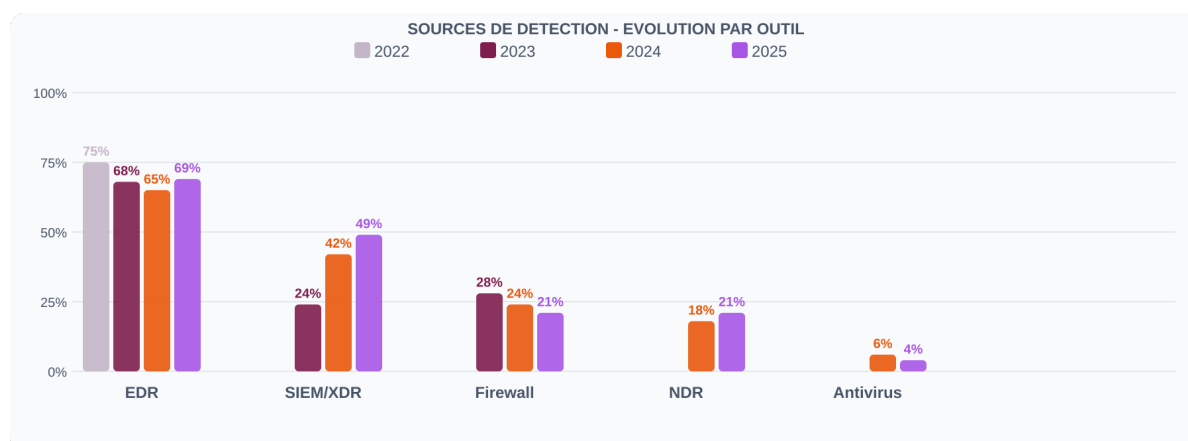
5 techniques les mieux détectées

- T1003 : OS Credential Dumping
- T1558 : Steal or Forge Kerberos Tickets
- T1562 : Impair Defenses
- T1548 : Abuse Elevation Control Mechanism
- T1078 : Valid Accounts, Default Accounts

5 techniques les moins bien détectées

- T1046 : Network Service Discovery
- T1087 : Account Discovery
- T1048 : Exfiltration Over Alternative Protocol
- T1567 : Exfiltration Over Web Service
- T1021 : Remote Services, Lateral Movement

2.3 Focus sur les sources de détection



Sources de détection par outil, évolution 2022–2025

L'EDR rebondit à 69 % : l'enrichissement systématique de ses configurations à partir des résultats de simulation, en particulier sur les vecteurs PowerShell et les techniques LotL, confirme que la visibilité endpoint reste la pierre angulaire de la détection moderne. Le SIEM/XDR poursuit sa montée en puissance à 49 % : le couplage EDR + SIEM/XDR s'impose comme standard chez les organisations matures. Le NDR progresse à 21 %, porté par la surveillance OT/ICS et du mouvement latéral.

Recommandations

- Enrichir la configuration EDR à partir des résultats de simulation, en priorité sur PowerShell et les techniques LotL.
- Consolider le couplage EDR + SIEM/XDR comme épine dorsale du dispositif de détection.
- Déployer le NDR sur les périmètres OT/ICS et cloud où l'EDR ne peut être le seul capteur.

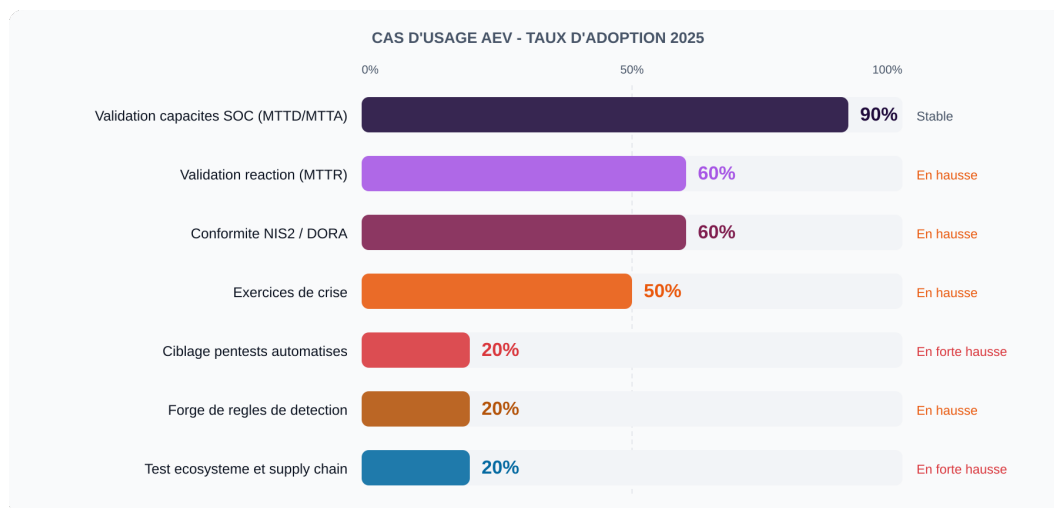
L'ESSENTIEL

La performance vient moins d'un outil isolé que de la façon dont les signaux sont croisés et les réponses enchaînées. À niveau d'outillage comparable, les organisations qui s'entraînent régulièrement progressent davantage que celles qui concentrent l'effort sur un test annuel.

3. L'AEV SE DÉPLOIE DANS LES ORGANISATIONS

3.1 Les cas d'usage observés

Le volume de simulations accumulé par BlackNoise permet cette année d'élargir l'analyse : aux résultats des simulations s'ajoute la façon dont les organisations les exploitent. L'AEV ne mesure pas seulement l'exposition, il pilote sa réduction.



Validation des capacités de détection — 90 %

Les indicateurs MTTD et MTTA sont devenus des KPI de pilotage présentés en comité de direction et intégrés aux contrats de service des MSSP. La simulation n'est plus un audit ponctuel : c'est un baromètre continu.

Validation de la réaction (MTTR) — 60 %, en hausse

Les organisations ne se contentent plus de détecter, elles chronomètrent leur capacité à réagir. Avant tout déploiement à large échelle, les contre-mesures activées par les EDR — kill de processus, suppression de fichiers, isolation de terminaux — sont validées en environnement réel pour s'assurer de leur efficacité et de l'absence d'effets de bord.

Conformité NIS2 / DORA — 60 %

L'AEV produit des indicateurs de vélocité, des scores cyber et des livrables de type TLPT. Le degré d'exploitation des vulnérabilités, issu de l'Automated Pentest, apporte un état des lieux des failles réellement exploitables.

Préparation aux exercices de crise — 50 % et plus

Plus d'une organisation sur deux utilise les simulations techniques pour alimenter ses exercices de gestion de crise : injects réalistes, test des chaînes d'alerte, vérification que les bons interlocuteurs sont joignables.

Ciblage des pentests, supply chain et forge de règles — 20 %

Les organisations s'appuient sur les données de simulation pour identifier les chemins d'attaque réellement exploitables avant de lancer un pentest, étendent leur périmètre aux partenaires et fournisseurs, et créent des règles calibrées sur leurs propres angles morts plutôt que d'appliquer des règles génériques. C'est l'application directe de la doctrine Response First.

3.2 L'entraînement des équipes : Human Readiness

Les simulations offrent un cadre d'entraînement unique : les analystes sont confrontés à des scénarios réels, dans leur environnement de production, avec leurs outils habituels.

Les logs, alertes et décisions d'une campagne permettent d'isoler la séquence qui a posé problème (signal ignoré, mauvaise qualification, escalade tardive, geste incomplet ou *playbook* inadapté...)



Comme en Formule 1, le simulateur permet de retravailler le secteur où la performance a chuté.

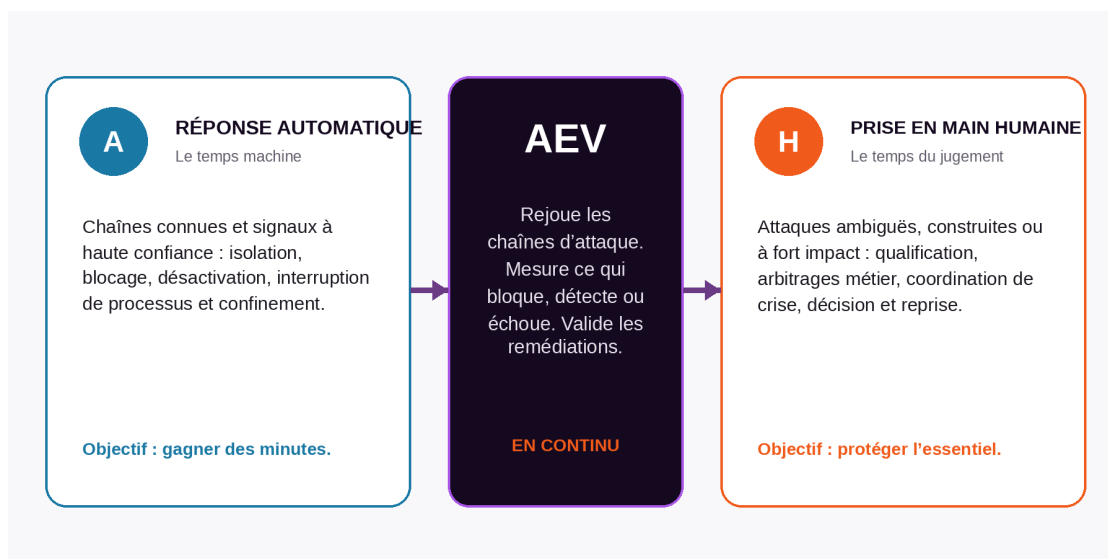
Cette séquence est transformée en un parcours de formation / sensibilisation court : replay technique, quiz, mise en situation, puis nouvelle simulation. Trois écarts reviennent systématiquement : des *playbooks* théoriques qui divergent de leur application réelle, une vélocité de qualification insuffisante, et des points uniques de défaillance dans la chaîne d'alerte — numéro d'astreinte invalide, mail tombant en spam, notification noyée dans les faux positifs.

L'ESSENTIEL

Intégrer les simulations AEV dans un programme d'entraînement structuré, à fréquence trimestrielle minimale sur les scénarios critiques, avec revue systématique des écarts *playbook*/réalité après chaque campagne.

4. UNE DÉFENSE À DEUX VITESSES

Sur les environnements sensibles ou transactionnels, quelques secondes suffisent à produire un impact. Les attaques graves exigent aussi des humains entraînés à reprendre la main.



L'AEV met à l'épreuve le temps machine comme le temps du jugement.

Sur les périmètres sensibles, industriels ou à fort impact transactionnel, une attaque coordonnée peut produire un effet métier avant la qualification humaine. Les plateformes XDR commencent à contenir automatiquement ces chaînes à partir de signaux corrélés multi-sources : elles réduisent le mouvement latéral et donnent du temps aux analystes.

La bonne frontière n'est pas « humain ou machine ». Elle sépare les actions répétables et à haute confiance des décisions ambiguës, à fort impact ou dépendantes du contexte métier.

L'ESSENTIEL

Activer le blocage automatique d'abord sur des scénarios à haute confiance et à fort impact, après validation en conditions réalistes, puis rejouer après chaque changement important.

5. PENTEST vs. AEV : PROFONDEUR ET CONTINUITÉ



L'AEV évite d'attendre le prochain pentest pour vérifier une correction ou une règle.

Ce que le pentest fait mieux

Créativité humaine, exploration d'enchaînements complexes avec un « touché humain », compréhension du contexte, démonstration ciblée d'un impact et regard expert sur les failles de conception.

Ce que l'AEV rend possible

Fréquence, couverture rejouable, mesure MTDD/MTTR, validation des contrôles de non-régression, intégration API et traitement massifié de la data, suivi des remédiations et ciblage des futurs tests experts.

L'ESSENTIEL

Automatiser l'exploration répétitive et la validation des remédiations ; concentrer le temps des pentesters sur les scénarios complexes justifiant une expertise humaine, les actifs critiques et les chemins réellement exploitables.

6. MISE EN ŒUVRE OBSERVEE SUR LE TERRAIN

Les scénarios gagnent en crédibilité quand ils produisent de vrais signaux, de vraies alertes et de vraies décisions.

Enrichir et crédibiliser les exercices de crise Cyber

Situation — L'organisation veut tester l'alerte, la qualification, l'escalade et la décision sans se limiter à un scénario papier.

Apport AEV — Une chaîne d'attaque est exécutée sur un périmètre contrôlé ; les équipes reçoivent des signaux réels et la cellule de crise travaille sur des éléments techniques crédibles.

Résultats — Chronologie, décisions, écarts *playbook*/réalité, MTTD/MTTR, plan de remédiation.

Préparer et déployer un programme de TLPT

Situation — Le test formel est rare, exigeant et fortement gouverné. Les équipes doivent progresser entre deux exercices, et démontrer une continuité de preuve entre-temps.

Apport AEV — L'AEV prépare les scénarios, teste les contrôles, facilite et automatise le Purple team et rejoue les remédiations, sans se substituer au Red team test prescrit.

Pour les entités financières désignées, DORA impose un TLPT au moins tous les trois ans ; le cadre TIBER-EU 2025 en précise les étapes. NIS2 porte la même attente de preuve et de continuité : en France, la transposition restait incomplète à l'été 2026, sans remettre en cause la nécessité de se préparer.

Résultats — Evidence pack, couverture MITRE, rapport d'exercice, preuves de replay, suivi des actions.

Valider les SLA d'un prestataire

Situation — Les SLA contractuels décrivent des délais, mais la chaîne de prise en charge reste peu testée.

Apport AEV — Campagnes répétées sur plusieurs plages horaires, avec suivi des acquittements, escalades et remédiations.

Résultats — MTTD/MTTA/MTTR, preuve de service, écarts de procédure, plan d'amélioration.

L'ESSENTIEL

Une seule campagne, plusieurs destinataires. Le SOC et le CERT exploitent les logs ; les équipes de gestion des vulnérabilités qualifient l'exploitabilité ; la GRC récupère la preuve ; le prestataire est évalué sur des résultats ; la crise dispose d'un scénario crédible. Le gain vient de la réutilisation de la même donnée.

7. TENDANCES

7.1 Du BAS à l'AEV : un changement de paradigme

Pendant trois ans, les rapports BlackNoise ont documenté l'évolution du BAS comme outil de mesure.

En 2025, cette catégorie technologique achève sa mue : le BAS est absorbé par l'Adversarial Exposure Validation. Le BAS mesurait ; l'AEV valide. Elle confirme de façon continue et automatisée la faisabilité réelle d'une attaque, son impact potentiel, et la capacité de l'organisation à la détecter, y réagir et s'en remettre. La convergence de ces composantes dans une plateforme unifiée fait passer d'une logique de test à une logique de pilotage continu de l'exposition.

7.2 Le ciblage offensif : Automated Pentest et ASM

En déléguant l'exploration systématique des chemins d'attaque à l'automatisation, les pentesters concentrent leur expertise sur les scénarios complexes : campagnes plus courtes, plus ciblées, ratio signal/bruit nettement amélioré. L'Automated Pentest confirme la compromission effective, pas seulement la simulation, et identifie précisément les vulnérabilités exploitables.

En amont, la *Hacker View Map* devient le point de départ des campagnes : avant de simuler une attaque, la question est de savoir par où entrerait un attaquant. L'ASM cartographie les actifs exposés sur Internet — domaines, IP, services, certificats, technologies — et nourrit directement les scénarios. Les chemins les plus réalistes partent d'expositions réelles, pas de périmètres hypothétiques.

7.3 Patch First et Response First

La croissance continue du nombre de vulnérabilités, aujourd'hui accélérée par l'IA offensive, rend la correction exhaustive hors d'atteinte. Le Patch First ne disparaît pas : il se complète par le Response First.

La réponse n'est pas d'abandonner le patching, mais de le compléter. Le Response First consiste à garantir en priorité une capacité de réaction sur les failles les plus exploitables dans le contexte de l'organisation : détecter l'exploitation, puis bloquer le processus, isoler l'hôte ou révoquer la session avant que l'attaquant n'atteigne son objectif. Le raisonnement est pragmatique : sur une faille critique, une réaction automatisée protège en quelques secondes, là où le déploiement du correctif sur l'ensemble du parc s'étale sur plusieurs heures, jours voire semaines.

La posture défensive intègre l'hypothèse qu'une partie des failles restera ouverte, et compense par une capacité de réaction à la hauteur — encore faut-il que cette capacité soit réelle, et non simplement configurée.

C'est précisément ce que l'AEV opérationnalise : rejouer les chemins d'attaque exploitant les failles prioritaires, vérifier que la chaîne détection-réaction se déclenche effectivement, mesurer le délai entre l'exécution et le blocage, et corriger ce qui ne se déclenche pas — avant qu'un attaquant n'emprunte le même chemin. Les 20 % d'organisations qui utilisent déjà l'AEV pour valider leurs règles et leurs automatismes de réponse sont les précurseurs d'un usage appelé à se généraliser.

7.4 Le R des xDR : l'automatisation du blocage s'accélère

La validation par simulation accélère l'activation des fonctions de blocage automatisé portées par les outils de défense modernes — le « R » de EDR, MDR, NDR et XDR. Tant que ces capacités ne sont pas validées, les organisations les maintiennent en mode détection seule, par prudence face aux faux positifs et aux effets de bord. L'AEV apporte la preuve que le blocage est fiable sur les scénarios testés, et lève la barrière psychologique du déploiement. Kill de processus, isolation de terminal, blocage de flux réseau se déclenchent en millisecondes, là où le MTTR humain se compte en minutes.

7.5 OT/ICS : une couverture qui s'élargit

Les environnements industriels représentent 12 % des campagnes en 2025, soit un doublement par rapport à 2024. Cette progression est tirée par la disponibilité croissante d'outils dédiés — NDR industriels, agents passifs, honeypots — et par la prise de conscience des directions, accélérée par NIS2. Ce que BlackNoise observe est cohérent avec les premières années du BAS sur les SI de gestion : taux de détection faibles, angles morts nombreux, équipes SOC peu familiarisées avec les TTP spécifiques aux protocoles industriels (Modbus, DNP3, OPC-UA).

7.6 Conformité NIS2, DORA, TIBER-EU : l'AEV comme preuve

La conformité réglementaire représente 60 % des cas d'usage AEV en 2025. Ce que les régulateurs demandent, et que l'AEV permet de produire, c'est de la preuve objective et continue : des données techniques démontrant que les mécanismes fonctionnent, à une fréquence documentée, avec des indicateurs de vélocité mesurables. Scores cyber par périmètre, évolution MTTD/MTTR, couverture des tactiques MITRE et rapports d'exercices constituent désormais des pièces à part entière des dossiers de conformité.

7.7 L'IA dans la détection et la remédiation

L'IA s'installe progressivement dans les chaînes de détection et de réponse. Sa valeur ne consiste pas à remplacer les analystes mais à automatiser les tâches répétitives : triage d'alertes, synthèse de logs, génération de requêtes, analyse de scripts. Le temps humain se réoriente vers les décisions où le jugement, le contexte et l'expérience comptent.

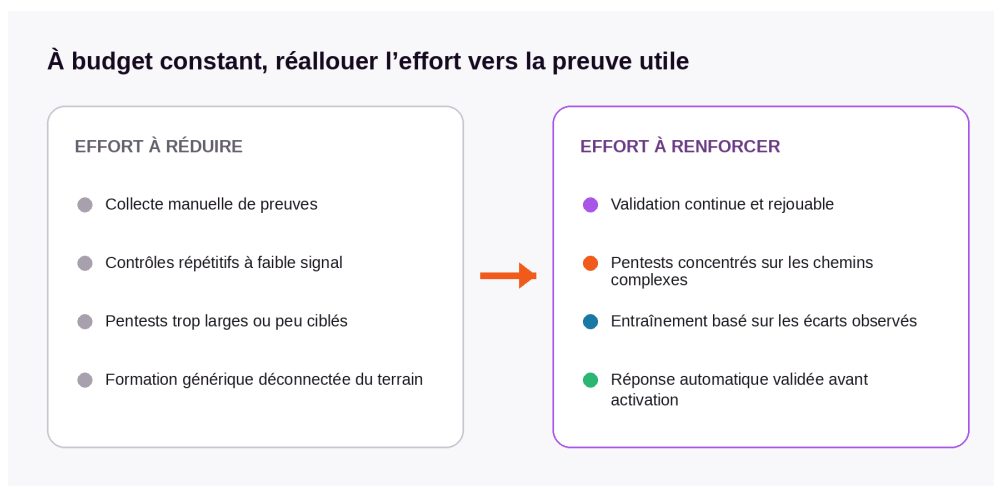
Ces apports doivent être mis en regard de limites significatives. Les modèles excellent sur le déjà-vu, peu sur l'émergent. Ils peuvent halluciner sans signal d'erreur explicite. Ils manquent du contexte propre à l'organisation. S'ajoutent les risques propres à l'IA elle-même : fuite de données, prompt injection, atrophie des compétences analystes. Et les attaquants intègrent aussi l'IA : phishing massif, deepfakes, code polymorphe.

L'ESSENTIEL

Plus les outils détectent, corrélient et bloquent automatiquement, plus il devient essentiel de tester ce qu'ils voient, ignorent ou interrompent réellement. C'est le rôle structurel de l'AEV dans un environnement défensif automatisé.

8. INVESTIR À BUDGET CONSTANT

La trajectoire la plus réaliste consiste souvent à déplacer du temps et des achats déjà engagés, pas à ajouter une couche de contrôle.



Principe de réallocation — à adapter au niveau de maturité et au modèle opérationnel.

Quatre leviers de ROI à budget constant

- **Preuve automatisée** — supprimer la collecte manuelle des éléments de conformité : les résultats sont rejouables et directement exploitables par la GRC.
- **Pentest ciblé** — concentrer le budget expert sur les chemins à forte valeur, au lieu de réexplorer les mêmes périmètres à chaque campagne.
- **Entraînement sur les écarts réels** — former et entraîner les analystes sur leurs défaillances constatées, plutôt que de financer des contenus génériques et des environnements de lab déconnectés.
- **Réponse automatique validée** — réduire le temps humain consacré aux actions répétitives de confinement, une fois le blocage automatique éprouvé.

L'ESSENTIEL

L'AEV rend visibles les doublons, les contrôles peu productifs et les endroits où un euro supplémentaire produit réellement un progrès.

9. CINQ RECOMMANDATIONS POUR 2026/2027

1. Qualifier les vulnérabilités ouvertes par les chemins d'attaque

Relier les failles non corrigées aux actifs critiques, à l'exploitabilité réelle et aux contrôles compensatoires par le renforcement de la détection.

2. Valider la réponse automatique

Tester isolation, blocage et désactivation avant activation large, puis après chaque changement majeur.

3. Entraîner la reprise en main

Choisir quelques scénarios à fort impact et rejouer la chaîne complète (SOC, métiers, direction, crise) pour assurer l'efficacité des processus de décision.

4. Transformer chaque écart en entraînement

Convertir les séquences faibles en replay technique, parcours ciblé, quiz ou mise en situation.

5. Réutiliser la même preuve

Alimenter SOC, CIRT, gestion des vulnérabilités, GRC, comité de direction, conformité, prestataires et plans de remédiation à partir des mêmes résultats.

EN CONCLUSION

Cette quatrième édition confirme que la validation de la sécurité opérationnelle est entrée dans l'âge adulte. La régularité prime sur l'exhaustivité : les organisations qui progressent le plus ne sont pas celles qui testent le plus largement, mais celles qui testent le plus souvent. Les angles morts se déplacent sans disparaître, et restent architecturaux plus que techniques.

L'AEV devient incontournable dès lors qu'il faut, avec des budgets contraints, démontrer l'efficacité opérationnelle, la conformité, la résilience et le maintien des compétences. Des investissements ciblés, une résilience démontrable.

SOURCES ET RÉFÉRENCES

Les données chiffrées proviennent des campagnes BlackNoise exécutées en 2025 et au premier semestre 2026, sauf mention contraire. Les séries d'évolution annuelle s'arrêtent à 2025, dernier exercice complet. Le contexte réglementaire et l'état de la menace sont arrêtés à l'été 2026.

- 1 Gartner, Market Guide for Adversarial Exposure Validation, 11 mars 2025.
- 2 Erium, Awards & Accolades, consulté en août 2026 : BlackNoise cité comme Representative Vendor dans la couverture Gartner de l'Adversarial Exposure Validation.
- 3 Google Cloud, Cloud Threat Horizons Report H1 2026 : la fenêtre entre divulgation d'une vulnérabilité et exploitation active est passée de semaines à quelques jours au second semestre 2025.
- 4 Google Cloud / Mandiant, AI Risk and Resilience, 9 mars 2026 : opérationnalisation de l'IA adverse, outils adaptatifs et agents opérant avec une supervision humaine minimale.
- 5 Microsoft Learn, Automatic attack disruption in Microsoft Defender, mise à jour du 23 juin 2026 : confinement en temps réel à partir de signaux XDR corrélés.
- 6 Banque centrale européenne, TIBER-EU Framework 2025 : alignement avec DORA, guidance de purple teaming, rapports et suivi des remédiations.
- 7 Règlement (UE) 2022/2554 (DORA), article 26, et règlement délégué (UE) 2025/1190 : TLPT au moins tous les trois ans pour les entités financières désignées.
- 8 Gartner, Top Cybersecurity Trends CISOs Must Act on in 2026, 17 mars 2026 : l'adoption d'agents IA dans le SOC exige un nouveau régime d'entraînement des analystes et des contrôles human-in-the-loop.
- 9 ENISA, NIS Investments 2025, 8 décembre 2025 : la conformité est le premier moteur d'investissement (70 %) ; 28 % des organisations mettent plus de trois mois à corriger les vulnérabilités critiques.
- 10 Commission européenne, 8 juillet 2026 : la France renvoyée devant la Cour de justice de l'Union européenne pour transposition incomplète de la directive NIS2.
- 11 Erium, communiqué du projet CYBAS / France 2030 : interopérabilité entre BlackNoise, HarfangLab, Gatewatcher, Snowpack et BreachHunt.

Gartner ne cautionne aucun fournisseur, produit ou service présenté dans ses publications. Ses travaux reflètent les opinions de son organisation de recherche et ne doivent pas être interprétés comme des déclarations de fait.

B|ACKNOISE



Direction de la publication : Pierre Texier (CTO Erium) ; Arnaud Le Men (CEO Erium)

erium.fr/blacknoise-aev | contact@blacknoise.co

Édité par le GroupeErium