Des milliers de constats à un plan de correction défendable

Vos scanners, évaluations cloud, tests applicatifs et revues des identités produisent des constats différents. L'accumulation peut masquer une chaîne courte : service exposé, privilège excessif et application métier accessible.

Nous rapprochons les résultats, supprimons les doublons et examinons accessibilité, privilèges et dépendances métier. Deep Advisor construit aussi des chemins d'attaque plausibles au-delà des scénarios connus, les confronte aux prérequis et associe des mesures correctives. Les analystes examinent les preuves avant chaque décision.

Partir des services plutôt que des volumes

Nous avons commencé par identifier les services et les actifs concernés, les points d'entrée et les responsables habilités à autoriser les changements. Les constats des scanners ont été rapprochés des applications, des chemins réseau et des identités afin de distinguer un défaut isolé d'un chemin pouvant réellement atteindre une activité.

Relier les résultats aux chemins d'attaque

Les doublons, composants obsolètes et alertes de configuration ont été rapprochés de leurs systèmes. Les analystes ont étudié les entrées, comptes de service, mouvements latéraux et contrôles compensatoires. L'évaluation Deep Advisor permet de proposer des enchaînements plausibles et de rattacher à chaque étape des mesures de correction.

Choisir les changements qui rompent plusieurs chemins

Une segmentation réseau ou un retrait de privilège peut interrompre plusieurs parcours. Les responsables ont comparé ces mesures avec les correctifs logiciels, les fenêtres de maintenance et les effets sur le service. Le plan d'action contient pour chaque décision les prérequis, les intervenants et les essais attendus.

De 4 000 constats à 14 éléments restants

Dans une mission de remédiation documentée menée par un expert senior, le registre opérationnel est passé d'environ 4 000 constats à 14 éléments restants au point de mesure retenu. Ce résultat associe analyse, responsabilisation, corrections et contre-vérifications. Le registre avant/après fait partie des preuves destinées à une évaluation approfondie.

Transmettre la décision et ses preuves

Chaque chemin prioritaire est relié au service, aux constats, à la correction, à son responsable, au retest et au suivi du risque résiduel. La direction dispose d'une synthèse tandis que les équipes conservent les données techniques reproductibles.

Réception et transmission

Votre équipe reçoit les chemins documentés, une vue avant/après, les responsables des corrections et les critères de vérification. Une mission de remédiation documentée a ramené le portefeuille opérationnel de 4 000 constats à 14 éléments restants.

Pour une évaluation cadrée : sales.advisor@deepinfosec.com.