DEEP INFOSEC / PUBLIC EVALUATION

Deep Advisor : relier les constats techniques à une décision de remédiation défendable

Évaluer la contextualisation des chemins d'attaque, la preuve, les responsabilités et la façon dont une correction change les priorités.

Exploiter les informations déjà disponibles

Le point de départ n'est pas le remplacement des scanners. L'équipe choisit des constats issus de la gestion des vulnérabilités, du cloud, de l'IAM, du code ou des outils de détection. L'évaluation précise les actifs, identités, privilèges et services métiers qui peuvent être reliés. Les sources de données sont convenues pour le projet : une catégorie d'intégration ne signifie pas qu'un connecteur particulier est certifié.

Montrer pourquoi la séquence change le risque

Un service d'administration accessible, un compte excessivement privilégié et une règle de segmentation imparfaite peuvent se retrouver dans trois files de traitement différentes. Deep Advisor examine s'ils forment un chemin vers un service critique. Chaque relation doit pouvoir être confrontée aux preuves, hypothèses et incertitudes. Les équipes comparent ensuite l'effet d'une suppression de privilège, d'une restriction réseau ou d'une correction de configuration.

Conduire la décision jusqu'à sa clôture

Le résultat attendu dépasse la carte de chaleur. Chaque chemin retenu relie l'impact métier, la preuve technique, les mesures possibles, le responsable, la vérification après correction et l'explication destinée au CISO ou au régulateur. Le pilote inclut des rapprochements trompeurs et des données incomplètes afin d'évaluer honnêtement la qualité du raisonnement.

Déroulement de l'évaluation

1. Choisir un service représentatif — On fixe le service métier, l'inventaire, les constats échantillons et les limites d'accès.

2. Construire puis contester les chemins — Un évaluateur technique examine les liens, les preuves manquantes et les explications bénignes.

3. Comparer les corrections — On mesure les changements de contrôle, leurs coûts d'exploitation et la rupture du chemin.

4. Examiner le dossier de décision — L'équipe évalue la reproductibilité et l'utilité des sorties pour dirigeants et ingénieurs.

Ce que vos équipes reçoivent

L’évaluation remet la carte des sources et identités, des chemins validés, un registre de remédiation hiérarchisé, les hypothèses du modèle, des décisions exécutives exemples et un protocole de contre-vérification.

Préparer une demande d’achat exploitable

Nous souhaitons évaluer Deep Advisor sur [service critique] à partir de [outils de scan/cloud/IAM/EDR]. Notre équipe suit environ [volume] constats et doit décider [question de remédiation]. Merci de proposer les limites d’accès, les livrables, les évaluateurs et le coût du pilote.

sales.advisor@deepinfosec.com