Réduire les risques qui menacent vos services essentiels en 90 jours

Vous disposez déjà d’outils, d’équipes et de plans de correction. La difficulté est d’identifier les combinaisons de failles qui menacent réellement une activité, de choisir les premières interventions et de prouver leur efficacité. Notre programme associe les responsables des services métier, les spécialistes cloud et IAM, nos ingénieurs et l’analyse de chemins d’attaque de Deep Advisor.

Jours 1 à 30 · Comprendre l’exposition réelle

Nous délimitons les services critiques, rapprochons les constats autorisés et cartographions dépendances et chemins d’attaque. Une ligne de base technique et métier est définie.

Jours 31 à 60 · Rompre les chemins les plus dangereux

Vos responsables valident les corrections avec nos architectes. Nous testons les mesures, ajustons les contrôles autorisés et privilégions les actions qui rompent plusieurs chemins d’attaque.

Jours 61 à 90 · Démontrer et transmettre

Nous vérifions l’efficacité des changements, documentons les preuves et remettons une synthèse de direction ainsi qu’une feuille de route exécutable.

Livrables et responsabilités

Vous recevez une carte des services critiques, un registre de chemins d’attaque, une vue risque/impact/reprise, le journal des décisions, les contrôles testés et un dossier de synthèse. Vos équipes valident les changements; nous assurons l’analyse, l’ingénierie et le transfert.

Premier engagement

Commencez par un service métier ou un portefeuille défini. Le programme peut ensuite alimenter un suivi continu avec Deep Advisor.

Notes de mise en œuvre

Choisir le premier périmètre

Sélectionner un service métier essentiel, ses responsables, dépendances et critères de réception. Définir les sources d’information, les fenêtres d’essai et les changements autorisés.

Mesures techniques et métier

Vérifier la joignabilité, les privilèges, les chemins d’attaque exploitables, les contrôles compensatoires, l’impact et la capacité de reprise.

Décider et tracer

Chaque chemin prioritaire est relié au service, à ses prérequis, au responsable de la correction, à la décision prise, aux tests et au risque résiduel.

Réception et suite

Recevoir le périmètre analysé, les contrôles exécutés ou différés, les contre-tests et la feuille de route attribuée aux responsables.

sales.advisor@deepinfosec.com | https://deepinfosec.com