DEEP INFOSEC / 90-DAY PROGRAMME

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.

30 / 60 / 90

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.

Périmètre initial de 90 jours

- Un service métier critique et son responsable identifié
- Jusqu’à trois sources de preuves autorisées : scanner, cloud ou identité
- Un périmètre technique IAM/architecture convenu et cinq hypothèses de chemins prioritaires au maximum
- Un chantier de correction choisi avec l’exploitant, ses contre-tests et le dossier de transmission à la direction

Équipes et responsabilités

- Deep InfoSec : pilotage, architecture, analyse des chemins et ingénierie de vérification prévue au contrat
- Votre organisation : responsable métier, accès, exports/connecteurs, validation des changements et réception
- Autres prestataires : changements sur les plateformes ou terrains placés sous leur autorité

Budget indicatif du programme de 90 jours

24 000–58 000 € HT · 25 à 45 jours de conseil répartis sur 90 jours

Réception et transmission

- Jour 30 : périmètre validé, dépendances, sources de preuves et chemins de référence
- Jour 60 : décisions, responsables, interventions et contrôles compensatoires
- Jour 90 : contre-tests, risques résiduels, procédures et synthèse de direction

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.

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