Plan 30 / 60 / 90 jours

Une trajectoire de renforcement cyber lisible par une direction, après un audit, une crise ou une exigence client/assurance. Chaque jalon relie une action à un risque, un responsable et une échéance.

0 – 30 JOURS
Stabiliser

- Cartographier actifs & risques prioritaires
- Corriger les vulnérabilités critiques exposées
- Activer l'authentification multifacteur (MFA)
- Vérifier et tester les sauvegardes
- Poser une gouvernance de crise (qui décide, qui alerte)

Responsable / échéance :

30 – 60 JOURS
Structurer

- Analyse de risques EBIOS RM (scénarios prioritaires)
- Politique SSI & gestion des accès (moindre privilège)
- Journalisation et supervision des événements
- Plan de remédiation priorisé et défendable
- Sécurité des prestataires & de la chaîne d'appro.

Responsable / échéance :

60 – 90 JOURS
Pérenniser

- PCA / PRA / BIA : activités critiques, RTO, RPO
- Exercice de crise / test de restauration
- Indicateurs & reporting cyber à la direction
- Trajectoire NIS 2 / DORA si concerné
- Revue et boucle d'amélioration continue

Responsable / échéance :

Besoin d'adapter ce plan à votre contexte réel ?
Forterys transforme cette trame en trajectoire priorisée et chiffrée.

forterys.com

Trame indicative : l'ordre et le contenu des jalons dépendent de votre secteur, de votre maturité et de vos contraintes opérationnelles.