Checklist : Transition vers la Cryptographie Post-Quantique

Cette checklist a été conçue pour aider les consultants et professionnels IT à évaluer l'état actuel de leurs systèmes de chiffrement et à initier des échanges structurés avec leurs clients sur la migration vers des solutions post-quantiques.

## 1. Évaluation des systèmes actuels de chiffrement

* ☐ Lister tous les points d'entrée utilisant le chiffrement (VPN, emails, stockage, etc.)
* ☐ Identifier les algorithmes utilisés (RSA, ECC, etc.)
* ☐ Vérifier les dates de validité des certificats TLS/SSL
* ☐ Identifier les systèmes critiques nécessitant un haut niveau de sécurité

## 2. Sensibilisation et documentation

* ☐ Préparer une synthèse claire sur la menace quantique et la stratégie 'Harvest Now, Decrypt Later'
* ☐ Fournir des exemples concrets sectoriels (santé, finance, administration publique)
* ☐ Comparer les algorithmes classiques et post-quantiques (Kyber, Dilithium, SPHINCS+)

## 3. Définition d’un plan de transition post-quantique

* ☐ Identifier les systèmes pouvant être mis à jour (vs legacy)
* ☐ Proposer une feuille de route progressive (ex : migration hybride)
* ☐ Anticiper les besoins réglementaires (RGPD, PCI-DSS, etc.)
* ☐ Planifier la montée en compétences (formations internes ou externes)

## 4. Communication avec le client

* ☐ Expliquer les risques en lien avec leur secteur d’activité
* ☐ Présenter une stratégie adaptée (court/moyen/long terme)
* ☐ Clarifier les avantages business : confiance, conformité, anticipation des risques