[TECH11]

- **Objectifs**
  - **Comprendre les principes fondamentaux de la PQC** (Post-Quantum Cryptography) et de la crypto-agilité, en mettant en évidence leurs enjeux et leurs applications
  - **Identifier les méthodes et bonnes pratiques pour intégrer la PQC et la crypto-agilité dans les architectures logicielles et les processus de développement**
  - **Savoir appliquer les concepts de la PQC et de la crypto-agilité dans la conception et l'évolution de systèmes logiciels** sécurisés et résilients face aux menaces quantiques

- **Public visé :** Architectes, développeurs, tech leads
- **Prérequis**
  - Connaissances du fonctionnement des équipements cryptographiques d'entreprise (PKI, CLM, HSM)
  - Connaissances de base de la cryptographie
  - Maîtrise de l'architecture de l'entreprise
  - Maîtrise de l'architecture logicielle

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Cyberdefense

Intégrer la cryptographie post-quantique et la crypto-agilité dans le développement logiciel

Programme de formation

- **Rappels fondamentaux de cryptographie**
  - Algorithmes symétriques vs asymétriques
  - Protocoles courants (TLS, PKI, etc.)
- **Menace quantique et impacts sur les SI**
  - Algorithmes menacés (RSA, ECC)
  - Scénarios d'attaque et "store now, decrypt later"
- **Algorithmes post-quantiques**
  - Présentation des familles (lattice, code-based, hash-based, multivariate, isogeny-based)
  - Focus sur les algorithmes à privilégier Critères de choix (sécurité, performance, compatibilité)
  - Intégration de la PQC dans les architectures
- **Solutions disponibles**
  - Solutions compatibles (hardware, software, open-source, propriétaire, ex: openSSL,...)
  - Considérations
- **Migration post-quantique**
  - Création de feuille de route
  - Le rôle des architectes et développeurs
- **Principes de la crypto-agilité**
  - Définition, enjeux, bénéfices
  - Patterns d'architecture crypto-agile
  - Découplage applicatif/crypto
  - Guidelines sur la crypto-agilité
- **Tests, validation et migration**
  - Stratégies de test (interopérabilité, performance, sécurité)
  - Plan de migration progressive
  - Plan de retour en arrière

[TECH11] Intégrer la cryptographie post-quantique et la crypto-agilité dans le développement logiciel

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques
- Exemples d'intégrations, analyse d'impacts sur la performance, exemples sur l'architecture
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	Français / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).