Cryptographie post-quantique : algorithmes NIST PQC et préparation à la transition

Lien : https://innov-systems.com/formation/cryptographie-post-quantique-algorithmes-nist-pqc-et-preparation-a-la-transition

DURÉE
5 jours (35h)

RÉFÉRENCE
SI83

CATÉGORIE
Sécurité Technique : Cryptographie, Protocoles et Infrastructures

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les impacts de l’informatique quantique sur la cybersécurité
- Maîtriser les principes de la cryptographie post-quantique
- Découvrir les algorithmes normalisés par le NIST
- Identifier les systèmes cryptographiques vulnérables
- Réaliser un inventaire des actifs cryptographiques
- Définir une stratégie de migration vers la cryptographie post-quantique
- Mettre en œuvre des approches hybrides de transition
- Intégrer les algorithmes PQC dans les infrastructures existantes
- Renforcer la crypto-agilité des systèmes d’information
- Anticiper les exigences réglementaires et normatives
- Réduire les risques liés à la menace quantique
- Étudier des cas concrets de transition vers la cryptographie post-quantique

POUR QUI ?

- Architectes cybersécurité
- Architectes d'entreprise
- Ingénieurs cybersécurité
- Architectes PKI
- Cryptographes
- RSSI / CISO
- Ingénieurs réseaux et télécommunications
- DevSecOps engineers
- Responsables de la gouvernance des systèmes d'information
- Consultants en cybersécurité
- Chercheurs et ingénieurs en cryptographie
- Toute personne impliquée dans la protection des infrastructures numériques et la transition vers la cryptographie post-quantique

Innov Systems

Programme détaillé

1 / Introduction à la cryptographie post-quantique

- Principes de l'informatique quantique
- Menaces des ordinateurs quantiques sur la cryptographie actuelle
- Enjeux de la transition vers la cryptographie post-quantique

2 / Fondamentaux cryptographiques

- Cryptographie symétrique et asymétrique
- Limites de RSA, Diffie-Hellman et ECC
- Impact des algorithmes de Shor et de Grover

3 / Standardisation des algorithmes NIST PQC

- Processus de sélection du NIST
- Algorithmes retenus pour la normalisation
- État de la standardisation et perspectives

4 / Algorithmes post-quantiques

- Cryptographie basée sur les réseaux (lattices)
- Cryptographie basée sur les codes correcteurs
- Autres familles d'algorithmes post-quantiques

5 / Signatures numériques post-quantiques

- Principes des signatures PQC
- Cas d'usage et intégration applicative
- Comparaison avec les signatures classiques

Innov Systems

6 / Échange de clés et chiffrement post-quantique

- Mécanismes d’établissement de clés
- Chiffrement hybride classique/PQC
- Migration progressive des infrastructures

7 / Inventaire cryptographique et stratégie de migration

- Cryptographic Asset Inventory
- Crypto-agilité et gestion du cycle de vie
- Feuille de route de transition

8 / Déploiement dans les infrastructures IT

- Intégration dans PKI, TLS et VPN
- Compatibilité avec les systèmes existants
- Contraintes de performance et d’interopérabilité

9 / Gouvernance, conformité et gestion des risques

- Recommandations des organismes de normalisation
- Politiques de sécurité et gouvernance cryptographique
- Gestion des risques liés à la transition PQC

10 / Cas pratiques et préparation à la transition

- Élaboration d'un plan de migration post-quantique
- Analyse d'une architecture d'entreprise
- Bonnes pratiques et retours d'expérience

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

08 au 12 Fév. 2027	Présentiel - Casablanca
05 au 09 Avr. 2027	Présentiel - Casablanca
31 Mai au 04 Juin 2027	Présentiel - Casablanca
26 au 30 Juil. 2027	Présentiel - Casablanca
20 au 24 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés