QC6 | La cybermenace quantique



Nouvelle formation

NIVEAU : DÉBUTANT

Publics : Cette formation s'adresse aux décideurs (dirigeants d'entreprises, dirigeants d'administration) et aux personnels en charge de la cybersécurité dans leur entité.

Prérequis : Aucun

Responsable(s) pédagogique(s) : Mathieu KLINGLER - Responsable Houko Formation, docteur en informatique

Langue de la formation : Français

Capacité maximum : 12

Prix : 900€ HT - **Durée :** 1 jour

Contexte

L'essor des communications numériques a fait de la cryptographie un élément indispensable au fonctionnement de notre société. En assurant la confidentialité, l'intégrité et l'authenticité des informations, elle est aujourd'hui omniprésente.

La confiance accordée à la cryptographie est toutefois remise en cause par l'avènement de l'informatique quantique. Contrairement aux ordinateurs classiques, un ordinateur quantique suffisamment puissant pourrait compromettre la sécurité des principaux algorithmes cryptographiques actuellement déployés, et par conséquent les garanties de sécurité sur lesquelles reposent nos systèmes d'informations.

Cette formation a été conçue pour sensibiliser à cette nouvelle menace et donner les bases de connaissance pour opérer la transition de nos systèmes d'information vers une cryptographie résistante à l'ordinateur quantique.

Objectifs

- Maitriser les concepts d'ordinateur quantique et de cryptographie.
- Comprendre la menace quantique et ses enjeux.
- Comprendre l'approche nécessaire pour réaliser une transition vers des solutions résistantes à la menace quantique.

QC6 | La cybermenace quantique

Thèmes abordés

Cryptographie,
Capacités d'un ordinateur quantique,
Impact d'un ordinateur quantique sur la cryptographie,
Cryptographie Post-Quantique

Le programme

Module #1 — Comprendre les enjeux de la transition post-quantique

1. La cryptographie
- Qu'est-ce que la cryptographie ?
- Où et comment est-elle utilisée ?
- L'ampleur de son utilisation et l'importance qu'elle joue dans notre société

2. L'ordinateur quantique
- Qu'est-ce qu'un ordinateur quantique ?
- Ses capacités et ses utilisations

3. L'impact de l'ordinateur quantique sur la cryptographie
- La vulnérabilité des systèmes actuels face à l'ordinateur quantique
- Les potentielles conséquences à court, moyen et long terme
- Les attaques « Récolter maintenant, déchiffrer plus tard »
- Qui et qu'est-ce qui est impacté ?

4. Les solutions disponibles
- La Cryptographie Post-Quantique
- La Cryptographie Quantique
- L'état de l'art

Module #2 — Comment se protéger et réaliser sa transition post-quantique

5. Le panorama réglementaire
- La standardisation de la Cryptographie Post-Quantique
- Les recommandations des agences de cybersécurité

6. L'approche globale d'une transition post-quantique

7. L'inventaire cryptographique et l'analyse des risques
- Qu'est-ce qu'un inventaire cryptographique ?
- Comment réaliser un inventaire cryptographique et comment l'utiliser
- L'analyse de risques

8. La protection des actifs
- Comment élaborer une roadmap de transition
- Les solutions existantes

9. Mise en pratique
- Exemple d'inventaire cryptographique
- Étude du cas de l'entreprise

Méthodologie et évaluation

Questionnaire de positionnement
Présentation, échange et cas pratiques présentés
Démonstrations interactives

QC6 | La cybermenace quantique

QCM en fin de formation

Formation Continue de l'Institut d'Optique - 2 av. Augustin Fresnel, 91127 Palaiseau. Tél . : +33 1 6453 3236 - fc.institutoptique.fr
PARIS-SACLAY - SAINT-ETIENNE - BORDEAUX