La cybersécurité et la blockchain

Programme *(Mis à jour le 20/11/2024)*

Introduction à la cybersécurité dans la blockchain (1h30)

- Comprendre les vecteurs d'attaque uniques aux blockchains et aux cryptomonnaies

Sécurité des Wallets et des Échanges (2h)

- Techniques de sécurisation des portefeuilles de cryptomonnaies et des plateformes d'échange

Vulnérabilités communes des smart contracts (2h15)

- Analyse des failles de sécurité les plus fréquentes dans les smart contracts

Ateliers de codage sécurisé (1h15)

- Techniques pour écrire des smart contracts sécurisés en Solidity et Vyper

Cryptographie appliquée à la blockchain (1h30)

- Utilisation de techniques cryptographiques avancées pour renforcer la sécurité des transactions blockchain

Implémentation de la confidentialité dans les transactions (2h)

- Techniques comme le zk-SNARKs et le Mimblewimble pour assurer la confidentialité et l'anonymat

Sécurisation des nœuds et des réseaux blockchain (2h15)

- Meilleures pratiques pour sécuriser les nœuds dans un réseau blockchain, y compris la gestion de l'accès et le monitoring

Simulation d'attaques et réponse aux incidents (1h15)

- Simulations de tentatives de piratage sur un réseau blockchain test pour pratiquer la réponse aux incidents

Audits de sécurité pour les applications blockchain (1h30)

- Comment réaliser des audits de sécurité internes et externes, choisir des auditeurs

Conformité réglementaire et blockchain (2h)

- Discussion sur les aspects légaux et réglementaires affectant la sécurité des blockchains

Développement d'une stratégie de sécurité blockchain (2h15)

- Création de politiques de sécurité qui intègrent la gestion des risques, la récupération après sinistre et la continuité des opérations

Atelier de politique de sécurité (1h15)

- Les participants créent une politique de sécurité pour une application blockchain fictive

Référence

THBI3303

Durée

3 jours / 21 heures

Prix HT / stagiaire

2265€

Objectifs pédagogiques

- Renforcer ses compétences en cybersécurité en lien avec la blockchain (règlementation, sécurité des contrats intelligents, protection des portefeuilles de crypto-monnaie).
- Savoir utiliser les différentes techniques disponibles pour garantir et sécuriser les accès aux données stockées (cryptographie, hash, architectures distribuées).
- Détecter et analyser les risques potentiels de sécurité et proposer des solutions adaptées en cas de faille de sécurité.

Niveau requis

- Avoir une première expérience en cybersécurité et/ou en cryptographie
- Connaître les langages de programmation spécifiques blockchain.

Public concerné

- Architectes blockchain
- Développeurs de protocole
- Développeurs de smarts contracts

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de l'évaluation des résultats de la formation

Feuilles d'émargement (signature électronique privilégiée)