EduGroupe
Accompagner pour réussir

La cybersécurité et la blockchain

Référence : **DEBC008** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Avoir une première expérience en cybersécurité et/ou en cryptographie . • 2-Connaître les langages de programmation spécifiques blockchain.

PROFIL DES STAGIAIRES

• Architectes blockchain, développeurs de protocole, développeurs de smarts contracts.

OBJECTIFS

• A l'issue de la formation, le stagiaire sera capable de sécuriser les programmes blockchain. • Plus précisément : • 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.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Blockchain

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1 - MATIN / Fondamentaux de la Cybersécurité Blockchain

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

JOUR 1 - APRES-MIDI / Sécurité des Smart Contracts

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

JOUR 2 - MATIN / Techniques de Cryptographie Avancées

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

JOUR 2 - APRES-MIDI / Réseaux Blockchain Sécurisés

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

JOUR 3 - MATIN / Audit et Conformité

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

JOUR 3 - APRES-MIDI / Stratégies de Sécurité Globale

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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.