Sécurité Blockchain

Durée: 3 Jours **Réf de cours: U67946G**

Résumé:

Ce cours exclusif sur la sécurité de la blockchain couvre tous les aspects connus de la sécurité de la blockchain qui existent aujourd'hui.
Ce cours fournit un aperçu détaillé de toutes les questions de sécurité de la Blockchain, y compris les menaces, l'atténuation des risques, l'intégrité de la sécurisation des nœuds, la confidentialité, les meilleures pratiques de sécurité, la sécurité avancée de la Blockchain et plus encore.
Les sessions de travaux pratiques approfondies fourniront aux participants des outils pratiques et réels pour non seulement reconnaître les menaces de sécurité, mais aussi leur atténuation et leur prévention.
Mise à jour : 15/11/2024

Public visé:

Security for Blockchain Professionals est conçu pour les architectes, les développeurs de logiciels, les administrateurs de systèmes et de réseaux qui sont responsables de la mise en œuvre, de l'identification et de la gestion de la sécurité sur leur réseau Blockchain.Il s'adresse aussi aux responsables qui doivent atténuer, reconnaître et résoudre les problèmes de sécurité de la Blockchain.
En raison de l'accent mis sur les méthodes techniques de cybersécurité et de la vaste portée de ce cours, les personnes ayant des connaissances actuelles en matière de cybersécurité, d'architecture de la Blockchain et/ou les programmeurs expérimentés tireront le plus grand bénéfice de ce cours, y compris les : Architectes Blockchain Développeurs de blockchain Développeurs d'applications Administrateurs de systèmes de blockchain Architectes de la sécurité des réseaux Experts en cybersécurité Professionnels de l'informatique avec expérience en cybersécurité

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Identifier et différencier les menaces de sécurité et les attaques sur un réseau Blockchain.
- Comprendre les méthodes de sécurité de la blockchain, les meilleures pratiques, l'atténuation des risques, etc.
- Répertorier tous les vecteurs de cyber-attaques connus (à ce jour) sur la Blockchain.
- Analyser les risques de sécurité d'un réseau Blockchain.
- Comprendre les caractéristiques et les risques de sécurité inhérents à la blockchain.
- Maîtriser les meilleures pratiques de sécurité pour les administrateurs de systèmes/réseaux Blockchain.
- Démontrer les techniques appropriées de sauvegarde des données de la Blockchain.

Pré-requis:

Test et certification

Professionnel certifié en sécurité de la blockchain (CBSP)

Contenu:

Jour 1 : Principes fondamentaux de la sécurité de la blockchain

Module 1 : Sécurité fondamentale de la blockchain

- Cryptographie pour la blockchain
- Brève introduction à la blockchain
- Hypothèses concernant la sécurité de la blockchain
- Limites de la sécurité fondamentale de la blockchain

Module 2 : Consensus dans la blockchain

- Consensus de la blockchain et généralités hasardeuses
- Introduction au consensus de la blockchain
- Preuve de travail
- Preuve d'enjeu
- Autres algorithmes de consensus de la blockchain

Module 3 : Mécanismes avancés de sécurité de la blockchain

- Mesures de sécurité liées à l'architecture
- Blockchains autorisées
- Points de contrôle
- Solutions cryptographiques avancées
- Signatures multipartites
- Preuves de notoriété nulle
- Adresses furtives
- Signatures en anneau
- Transactions confidentielles

Module 4 : Sécurité des Smart Contracts

- Introduction aux Smart Contracts
- Considérations sur la sécurité des Smart Contracts
- Audit du code des Smart Contracts

Jour 2 : Mise en œuvre de la sécurité de la blockchain

Module 5 : Évaluation des risques liés à la blockchain

- Considérations sur les risques liés à la blockchain
- Exigences réglementaires
- Conception architecturale de la blockchain

Module 6 : Sécurité de base de la blockchain

- Sécurité de l'utilisateur
- Sécurité des nœuds
- Sécurité du réseau

Module 7 : Blockchain pour les entreprises

- Introduction à la sécurité d'Ethereum
- Introduction à la sécurité Hyperledger
- Introduction à la sécurité de Corda

Module 8 : Mise en œuvre sécurisée des blockchains d'entreprise

- Opérations professionnelles
- Gestion des données
- Infrastructure
- Conformité légale et réglementaire

Jour 3 : Vulnérabilités de sécurité connues et solutions

Module 9 : Vulnérabilités et attaques au niveau du réseau

- 51% Attaques
- Attaques par déni de service
- Attaques par éclipse
- Attaques de rediffusion
- Attaques de routage
- Attaques Sybil

Module 10 : Vulnérabilités et attaques au niveau du système

- Le piratage de Bitcoin
- Le piratage de The Verge
- La vulnérabilité d'EOS
- La vulnérabilité de Lisk

Module 11 : Vulnérabilités et attaques des contrats intelligents

- Réentrance
- Contrôle d'accès
- Arithmétique
- Valeurs de retour non vérifiées
- Déni de service
- Mauvais fonctionnement aléatoire
- Conditions de concurrence (Race Conditions)
- Dépendance vis-à-vis de l'horodatage
- Adresses courtes

Module 12 : Sécurité des architectures DLT alternatives

- Introduction aux DLT basés sur des DAG
- Avantages des DLT basés sur un DAG
- Limites des DLT basés sur des DAG

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Un support de cours officiel sera remis aux stagiaires.
Pour les cours en présentiel : Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions.
Pour les cours en distanciel : Suivi de cette formation à distance depuis un site client équipé. Il suffit d'avoir une bonne connexion internet, un casque avec micro et d'être dans un endroit au calme pour en profiter pleinementUne fiche explicative est adressée en amont aux participants pour leur permettre de vérifier leur installation technique et de se familiariser avec la solution technologique utilisée.
L'accès à l'environnement d'apprentissage, ainsi qu'aux feuilles d'émargement et d'évaluation est assuré.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de