

Sécurité Blockchain

Durée: 3 Jours **Réf de cours: U67946G** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires sur tous les aspects connus de la sécurité de Blockchain qui existent dans l'environnement Blockchain aujourd'hui. Elle fournit un aperçu détaillé de toutes les questions de sécurité Blockchain, y compris les menaces, l'atténuation des risques, l'intégrité de la sécurité des nœuds, la confidentialité, les meilleures pratiques de sécurité, la sécurité Blockchain avancée et plus encore. Les sessions de labs approfondies fourniront aux participants des outils pratiques et réels non seulement pour reconnaître les menaces de sécurité, mais aussi pour les atténuer et les prévenir.

Mise à jour : 7.06.2023

Public visé:

Architectes, développeurs de logiciels, administrateurs système et réseau existants qui sont responsables de la mise en œuvre, de l'identification et de la gestion de la sécurité sur leur réseau Blockchain. De même, ceux qui sont responsables et doivent atténuer, reconnaître et résoudre les problèmes de sécurité des blockchains. Les étudiants participeront à des laboratoires de sécurité qui approfondiront les meilleures pratiques de sécurité, les vecteurs d'attaque connus, l'identification des menaces, les techniques de réponse, et bien plus encore. 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 Blockchain et/ou les programmeurs expérimentés tireront le plus grand profit de ce cours, notamment : Architectes, développeurs Blockchain et d'applications, administrateurs système de blockchain, architectes de la sécurité des réseaux, experts en cybersécurité et professionnels de l'informatique ayant une expérience de la cybersécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
 - Réaliser une analyse des risques de sécurité du réseau Blockchain.
- Identifier et différencier les menaces de sécurité et les attaques sur un réseau Blockchain.
 - Découvrir les caractéristiques et les risques de sécurité inhérents à la Blockchain.
- Expliquer les méthodes de sécurité Blockchain, les meilleures pratiques, l'atténuation des risques, et plus encore.
 - Expliquer les meilleures pratiques de sécurité pour les administrateurs de systèmes/réseaux Blockchain.
- Appréhender tous les vecteurs de cyber-attaque connus (à ce jour) sur la Blockchain.
 - Démontrer les techniques appropriées de sauvegarde des données de Blockchain.

Test et certification

Professionnel certifié en sécurité des chaînes de blocs (CBSP)

Contenu:

Jour 1

Principes fondamentaux de la sécurité des chaînes de blocs

Module 1 : Sécurité fondamentale de la blockchain

- Cryptographie pour la blockchain
- Une brève introduction à la blockchain
- Hypothèses sur la sécurité de la blockchain
- Limites de la sécurité de base de la blockchain

Module 2 : Consensus dans la blockchain

- Consensus de la blockchain et généraux byzantins
- Introduction à la sécurité du consensus de la blockchain
- Preuve de travail
- Preuve de l'enjeu
- Autres algorithmes de consensus de la blockchain

Module 3 : Mécanismes avancés de sécurité des blockchains

- Mesures de sécurité architecturales
- Blockchains à autorisation
- Checkpointing
- Solutions cryptographiques avancées
- Signatures multipartites
- Preuves de connaissance zéro
- Adresses furtives
- Signatures en anneau
- Transactions confidentielles

Module 4 : Sécurité des contrats intelligents

- Introduction aux contrats intelligents
- Considérations sur la sécurité des contrats intelligents
- Audit du code des contrats intelligents

Jour 2

Implémentations de la sécurité des blockchains

Module 5 : Évaluation des risques liés aux chaînes de blocs

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

Module 6 : Sécurité de base de la blockchain

- Sécurité des utilisateurs
- 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 commerciales
- 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% des attaques
- Attaques par déni de service
- Attaques Eclipse
- Attaques de relecture
- Attaques de routage
- Attaques Sybil

Module 10 : Vulnérabilités et attaques au niveau du système

- Le piratage de Bitcoin
- Le piratage de Verge
- La vulnérabilité EOS
- Vulnérabilité de Lisk

Module 11 : Vulnérabilités et attaques des contrats intelligents

- Réentraînement
- Contrôle d'accès
- Arithmétique
- Valeurs de retour non vérifiées
- Déni de service
- Mauvais aléatoire
- Conditions de course
- Dépendance vis-à-vis de l'horodatage
- Adresses courtes

Module 12 : Sécurité des architectures DLT alternatives

- Introduction aux DLT basés sur les DAG
- Avantages des DLT basés sur des DAGs

Limites des DLT basés sur des DAGs

Méthodes pédagogiques :

Support de cours remis aux participants

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'embarquement par demi-journée de présence est signée par tous les participants et le formateur.
- Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
- Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques