Cybersécurité & blockchain

3 j (21 heures) Ref : IABC004

Public

RSSI (Responsables Sécurité des SI) et responsables cybersécurité souhaitant comprendre et appliquer les principes de cybersécurité et blockchain dans leurs organisations

Pré-requis

Connaissances de base en sécurité informatique et en cryptographie
Familiarité avec les concepts de la blockchain et des registres distribués
Expérience en administration système ou développement logiciel recommandé

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Nombreux exercices pratiques et mises en situation, échanges basés sur la pratique professionnelle des participants et du formateur, formation progressive en mode participatif. Vidéoprojecteur, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Attestation de fin de formation

La formation "Cybersécurité & Blockchain" est un programme intensif de trois jours conçu pour les professionnels de l'informatique et de la sécurité qui souhaitent approfondir leurs connaissances en matière de sécurité des technologies blockchain. Cette formation explore les concepts de base et avancés de la cybersécurité appliqués à la blockchain, les types de menaces spécifiques, les techniques de protection et les meilleures pratiques pour sécuriser les infrastructures blockchain. Les participants apprendront à identifier et à atténuer les vulnérabilités, à comprendre les attaques courantes et à implémenter des mesures de sécurité efficaces.

Cette formation de trois jours offre une couverture complète des aspects critiques de la cybersécurité appliquée à la blockchain, permettant aux participants de devenir des experts capables de sécuriser efficacement des infrastructures et des applications blockchain contre les menaces et les vulnérabilités.

Objectifs

Comprendre les principes de base de la blockchain et leur impact sur la sécurité
Identifier et évaluer les menaces et les vulnérabilités spécifiques aux technologies blockchain
Appliquer les meilleures pratiques de sécurité pour protéger les infrastructures blockchain

Mettre en œuvre des techniques de cryptographie avancées pour sécuriser les transactions et les données

Analyser et répondre aux attaques contre les systèmes blockchain

Développer des stratégies de gestion des risques et de conformité pour les projets blockchain

Programme détaillé

INTRODUCTION A LA BLOCKCHAIN ET SECURITE DE BASE

INTRODUCTION A LA BLOCKCHAIN

Dans cette section introductive, nous abordons les fondamentaux de la blockchain en rappelant ses principaux concepts : décentralisation, consensus et immutabilité. La blockchain est une technologie distribuée qui permet la création d'un registre sécurisé et transparent des transactions. Elle élimine le besoin d'intermédiaires en utilisant des mécanismes de consensus pour valider et enregistrer les transactions de manière sécurisée et vérifiable. Les smart contracts, programmes autonomes exécutés sur la blockchain, permettent d'automatiser et de sécuriser l'exécution d'accords numériques.

PRINCIPES DE BASE DE LA CYBERSECURITE POUR LA BLOCKCHAIN

Nous explorons ici les principes fondamentaux de la sécurité informatique appliqués à la blockchain, notamment la CIA : Confidentialité, Intégrité et Disponibilité. La blockchain introduit de nouvelles perspectives en matière de sécurité en transformant la confiance traditionnelle en une confiance algorithmique et en permettant des échanges de valeur sans nécessiter de tiers de confiance centralisé. Cela impacte les modèles de sécurité traditionnels en renforçant la résilience face aux attaques malveillantes et en facilitant la traçabilité des transactions.

CRYPTOGRAPHIE ET BLOCKCHAIN

La cryptographie joue un rôle crucial dans la sécurisation des transactions et des données au sein des blockchains. Nous examinons les techniques cryptographiques clés utilisées, telles que le hashage pour assurer l'intégrité des données, les signatures numériques pour l'authentification des participants et le chiffrement asymétrique pour sécuriser les échanges de données sensibles. Ces techniques garantissent que les transactions sont sécurisées, vérifiables et résistantes à la falsification.

ATELIER PRATIQUE

Pour mettre en pratique les concepts étudiés, les participants implémentent des fonctions cryptographiques dans des transactions blockchain simulées. Cela inclut la génération de clés, la création de signatures numériques et la vérification d'intégrité des données. L'atelier se concentre également sur l'analyse de la sécurité des transactions réalisées sur une blockchain publique, mettant en lumière les défis spécifiques et les précautions nécessaires.

MENACES, VULNERABILITES ET TECHNIQUES DE PROTECTION

MENACES ET VULNERABILITES SPECIFIQUES A LA BLOCKCHAIN

Nous passons en revue les menaces courantes auxquelles les blockchains sont confrontées, telles que les attaques de type 51%, les attaques Sybil, la reentrancy et le double spending. À travers l'étude de cas de failles de sécurité célèbres comme celles du DAO et de Mt. Gox, nous explorons les conséquences de ces vulnérabilités et les leçons tirées pour renforcer la sécurité des systèmes blockchain.

SECURISATION DES SMART CONTRACTS

Les smart contracts présentent des risques uniques en raison de leurs vulnérabilités spécifiques. Nous discutons des bonnes pratiques de codage, telles que la gestion prudente des états, l'utilisation de modificateurs pour contrôler les autorisations d'accès et la gestion des erreurs de manière sécurisée. Cette approche proactive vise à minimiser les risques de bugs et à renforcer la fiabilité des smart contracts dans un environnement blockchain.

OUTILS DE SECURITE POUR LA BLOCKCHAIN

Nous introduisons des outils avancés tels que MythX, Slither et Remix, qui sont utilisés pour auditer et sécuriser les smart contracts. Ces outils permettent de détecter efficacement les vulnérabilités potentielles et de les corriger avant le déploiement sur la blockchain. L'accent est mis sur l'importance de l'audit régulier et de l'amélioration continue des pratiques de sécurité pour maintenir l'intégrité des systèmes blockchain.

ATELIER PRATIQUE

Les participants s'engagent dans des activités pratiques d'audit et de correction de smart contracts en utilisant les outils de sécurité mentionnés. Des démonstrations de tests de pénétration sur des applications décentralisées illustrent la façon dont les attaques peuvent être simulées et prévenues grâce à une préparation adéquate et à l'utilisation judicieuse des outils de sécurité disponibles.

GESTION DES RISQUES ET REPONSE AUX INCIDENTS

GESTION DES RISQUES POUR LES PROJETS BLOCKCHAIN

L'identification proactive des risques spécifiques aux projets blockchain est essentielle pour développer des stratégies de gestion des risques efficaces. Nous explorons les méthodes pour évaluer les risques potentiels, définir des mesures d'atténuation et élaborer des plans de réponse aux incidents. Cela inclut la surveillance continue et l'adaptation des stratégies en fonction des évolutions du paysage de la sécurité blockchain.

CONFORMITE ET REGLEMENTATION

Nous examinons les exigences réglementaires actuelles et émergentes pour les projets blockchain, notamment en ce qui concerne la protection des données, la confidentialité financière et la conformité fiscale. La mise en œuvre de politiques de conformité et de gouvernance robustes est cruciale pour assurer la conformité réglementaire et minimiser les risques juridiques potentiels.

REPONSE AUX INCIDENTS ET RECUPERATION

Les techniques de détection proactive des incidents et de réponse rapide sont essentielles pour minimiser les impacts des attaques sur les systèmes blockchain. Nous explorons les meilleures pratiques pour la gestion des incidents de sécurité, y compris la mise en œuvre de plans de récupération post-incident et la résilience des systèmes blockchain face aux perturbations.

ATELIER : Simulations d'incidents de sécurité et exercices de réponse.

Les participants se familiarisent avec le processus de développement de plans de réponse aux incidents pour différents scénarios, en mettant l'accent sur la coordination d'équipes multidisciplinaires et la mise en pratique des meilleures pratiques de sécurité blockchain.

SESSION DE CLOTURE : SYNTHESE ET Q&R

Récapitulatif des Concepts et des Techniques Appris

La session finale offre l'occasion de revoir les concepts abordés et de discuter des meilleures pratiques pour continuer à améliorer la sécurité dans les projets blockchain. Les participants sont encouragés à poser des questions et à échanger des idées avec les formateurs pour enrichir leur compréhension et envisager des applications futures des technologies blockchain sécurisées.