Les fondamentaux de la cybersécurité et de la blockchain

Date et durée

Code formation : SSR005FR
Durée : 3 jours
Nombre d'heures : 21 heures

Description

La cybersécurité est un enjeu majeur pour toutes les organisations, tandis que la blockchain se positionne comme une technologie d'avenir pour la sécurisation des données. Cette **formation intensive de 3 jours** est conçue pour vous fournir une introduction complète aux fondements de ces deux domaines.

Le programme vous guidera à travers les **fondamentaux de la cybersécurité**, de la typologie des menaces (phishing, ransomware) et aux principes de sécurité informatique (confidentialité, intégrité). Il abordera ensuite les normes et les bonnes pratiques, avant de vous initier à **la blockchain et ses liens avec la sécurité**. Des ateliers pratiques viendront ponctuer votre apprentissage pour une application concrète des concepts.

À l'issue de cette formation, vous serez capable d'identifier les menaces, de **comprendre les mécanismes de protection**, d'expliquer le fonctionnement de la blockchain et d'évaluer ses cas d'usage sécurisés. Vous saurez également appliquer les bonnes pratiques de sécurité dans divers environnements numériques.

Objectifs

À l'issue de cette formation en cybersécurité et blockchain, vous atteindrez les objectifs de compétences suivants :

- identifier les vecteurs d'attaque et les vulnérabilités critiques les plus courants dans un système d'information ;
- expliquer les principes fondamentaux et les mécanismes de défense (contrôle d'accès, chiffrement, supervision, etc.) pour sécuriser un système d'information ;
- décrire l'architecture, le consensus et le cycle de vie d'une transaction au sein d'une blockchain ;
- évaluer la pertinence d'une solution blockchain dans un cas d'usage donné et justifier son intégration dans une architecture sécurisée ;
- appliquer un référentiel de bonnes pratiques (hygiène numérique, gestion des clés, sauvegardes, conformité réglementaire) dans différents environnements (cloud, entreprise, mobilité et IoT).

Points forts

- **Approche pédagogique intensive** : bénéficiez d'une formation qui offre une introduction complète aux fondamentaux de la cybersécurité et de la blockchain.
- **Mise en pratique interactive** : maitrisez les concepts grâce à des ateliers pratiques qui viendront renforcer vos acquis théoriques.
- **Acquisition de compétences clés** : le contenu de la formation est conçu pour vous permettre de comprendre les enjeux de la sécurité informatique, les menaces actuelles, et les principes de fonctionnement de la blockchain et de ses applications sécurisées.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Bases en informatique** : maîtriser les concepts fondamentaux (systèmes d'exploitation, fichiers, processus et permissions).
- **Culture réseaux & systèmes** : connaître les notions essentielles (IP, DNS, TCP/UDP, pare-feu, client/serveur).

Public

Cette formation s'adresse aux publics suivants :

- Les **professionnels de l'informatique** (développeurs, administrateurs, analystes) qui souhaitent se familiariser avec les fondamentaux de la cybersécurité et la technologie blockchain pour mieux sécuriser leurs projets et infrastructures.
- Les **responsables sécurité** qui désirent mieux comprendre les principes de la blockchain et d'évaluer ses cas d'usage potentiels pour la protection des données et des systèmes.
- Les **recruteurs IT** qui souhaitent acquérir une meilleure compréhension des compétences techniques et des profils liés à la cybersécurité et à la blockchain afin de mieux cibler leurs recherches.
- Toute **personne intéressée** par la cybersécurité et la blockchain qui souhaite acquérir les bases théoriques et pratiques pour aborder ces sujets complexes.

Programme

Module 1 : comprendre les fondamentaux de la cybersécurité

- Les définitions, les enjeux et le panorama des menaces.
- Les acteurs clés de la cybersécurité.

Module 2 : analyser les types d'attaques et les vulnérabilités

- Les différents types d'attaques : phishing, ransomware, DDoS et malware.
- Les vulnérabilités critiques : failles logicielles, mauvaises configurations et vecteurs d'exploitation.

Travaux pratiques

- Cartographier des vulnérabilités d'un serveur web et analyser un incident de sécurité.

Module 3 : sécuriser les systèmes et les données

- Les principes de la sécurité informatique : confidentialité, intégrité et disponibilité.
- Les mécanismes de protection : authentification, chiffrement et pare-feu.

Module 4 : appliquer les normes et les bonnes pratiques

- Les normes et cadres de référence : ISO 27001, RGPD et NIST.
- La gestion des accès et des identités dans le cloud, la mobilité et l'IoT.

Travaux pratiques

- Mettre en place un plan de sécurité simple pour un environnement cloud hybride.

Module 5 : s’initier à la blockchain et à la sécurité

- Le fonctionnement de la blockchain : consensus, transactions et chaîne de blocs.
- Les différents types de blockchain (publique et privée).
- Les smart contracts et la cryptographie.

Module 6 : évaluer la sécurité dans la blockchain et ses cas d’usage

- Les cas d’usage de la blockchain : traçabilité, identité numérique et sécurité des données.
- Les limites et les risques liés à la blockchain : attaque des 51 %, faille de smart contract et oracle.

Travaux pratiques

- Démontrer un smart contract sécurisé et décider à l’aide d’une grille d’évaluation, si une blockchain est pertinente pour un projet donné.