La cybersécurité et les nouvelles technologies, perfectionnement

Cours Pratique de 3 jours - 21h
Réf : NYP - Prix 2024 : 2 390CHF HT

Vous avez suivi une initiation aux vulnérabilités sur les données tant dans le monde big data que dans l'embarqué. Nous vous proposons d'approfondir ces connaissances, d'analyser la sécurité de la blockchain, du cloud, de certains systèmes sensibles et de mieux cerner la cybersécurité dans son ensemble.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Maîtriser les enjeux de la cybersécurité des nouvelles technologies

Connaître les bonnes pratiques de la cybersécurité appliquées aux nouvelles technologies

Connaître les menaces pesant sur la blockchain

Connaître les menaces pesant sur le cloud et le big data

MÉTHODES PÉDAGOGIQUES

Pédagogie active, exposés, réflexions collectives, échanges interactifs.

EXERCICE

Chaque nouveau concept théorique est suivi de mise en pratique.

LE PROGRAMME

dernière mise à jour : 01/2024

1) Rappels de la cryptologie, la blockchain historique

- Cryptologie de base pour la blockchain.
- Différents algorithmes de hachage.
- La blockchain historique : le bitcoin.
- Consensus par minage.
- Le bitcoin en chiffres et en images.

Echanges : La cryptologie, la blockchain.

2) Attaques et défense dans la blockchain

- Sécurité blockchain vs cloud.
- Blockchain et sécurité de l'IoT (Internet des objets).
- Blockchain et vérification d'identité. Blockchain et supply chain.
- Vulnérabilités communes.
- Solidity, le langage des smart contracts.
- Hyperledger, la plateforme open source de développement de blockchain.
- La sécurité des développements des smart contracts (langage, méthodologie, vérification).
- Meilleures pratiques de sécurisation de la blockchain.

Travaux pratiques : Analyser la sécurité.

3) La "blockchain" Hyperledger

- Principes et terminologie.
- Différents types de nœuds.
- Architecture des services.
- Confidentialité des opérateurs.

PARTICIPANTS

Responsables et architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Connaissances en réseaux et systèmes. Avoir suivi la formation "La cybersécurité et les nouvelles technologies, initiation" ou posséder un niveau équivalent.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Les bases de Go, le langage des smart contracts.
Travaux pratiques : Construction d'une blockchain et premiers tests en Go.

4) Menaces sur le cloud computing

- Évaluation et gestion des risques du cloud par la norme ISO 27005.
- Les spécificités de la gestion des risques dans le cloud.
- Les principaux risques identifiés par l'ENISA.
- Comprendre l'analyse de sécurité.
- Outils de sécurité cloud.
Travaux pratiques : Analyse de sécurité sur Amazon Web Services EC2.

5) Menaces sur le big data

- Les solutions de stockage : HDFS, BDD NoSQL, Hadoop, HBase, MongoDB…
- Les architectures utilisées.
- Les différentes vulnérabilités.

6) Les vulnérabilités des systèmes

- Les botnets : comment sont-ils créés ?
- Les vulnérabilités de la domotique : caméras de surveillance, alarmes, TV, serrures connectées…
- Les vulnérabilités et attaques sur les réseaux WiFi.
- Les attaques par malware visant les micro-ordinateurs, tablettes et smartphones : drive-by download…
- Les bonnes pratiques de sécurisation de ces systèmes.
Travaux pratiques : Analyser la sécurité.

LES DATES

CLASSE À DISTANCE
2024 : 10 juin, 04 nov.