Domaine : Informatique - **Thématique(s) :** Cloud, réseaux et sécurité

STAGES COURTS

CYBERSÉCURITÉ : DÉVELOPPEMENT DE LOGICIELS SÉCURISÉS

Développer des logiciels sûrs est une tâche particulièrement complexe même pour un développeur d'applications averti. Elle nécessite une veille technologique constante à cause de l'évolution rapide de l'environnement d'applications (web,mobile, ...). La formation permet aux développeurs d'acquérir la méthodologie d'analyse des besoins et de conception et de préserver les exigences de sûreté tout au long du processus de développement ainsi que les mécanismes, les techniques et les outils de programmation sûre pour assurer la sécurisation des logiciels.

Durée de la formation : 35 heures
Dates : Voir le calendrier
Lieu : Campus Pierre et Marie Curie – Paris (Jussieu)
Tarif : 3300 €

Modalité : Présentiel

OBJECTIFS ET COMPÉTENCES VISÉES

L'objectif de cette formation est de présenter quelques méthodes et techniques permettant d'analyser et/ou de contrôler les flots d'information engendrés par les changements d'états d'un système ou lors de l'exécution d'un programme afin de garantir des propriétés de sécurité sur les données manipulées.
Et par conséquent, de fournir les connaissances aux apprenants pour assurer une intégration efficace des besoins et des exigences de sécurité dans tout projet applicatif, de maîtriser les activités liées à la sécurité applicative et de garantir la sécurisation des applications migrants.

PUBLIC VISÉ ET PRÉ-REQUIS

Public :
Formation destinée à des informaticiens ayant une expérience professionnelle d'au moins 5 ans dans les domaines de développement des logiciels ainsi qu'en systèmes d'information (SI).
Des connaissances d'assemblage et de configuration des composants matériels ou logiciel en respectant les standards en différentes technologie et en sécurité sont nécessaires.
Pré-requis :
Connaissances en programmation fonctionnelle, impérative, distribuée, web.

- Maitrise de cycle de vie des logiciels.
- Capacités d'abstraction.

PROGRAMME

- Présentation des vulnérabilités dans les langages de programmation
- Éléments de sémantique opérationnelle des langages de programmation
- Modèles de sécurité : contrôle d'accès versus contrôle de flots.
- Étude de cas : interprétation en termes de flots d'information des politiques de contrôle d'accès discrétionnaires (DAC) et à basée sur des treillis de niveau de sécurité
- Contrôle des flots d'information.

RESPONSABLE(S) PÉDAGOGIQUE

Mathieu Jaume

INFORMATIONS

Catégorie de l'action de développement des compétences:
(Article L6313-1 du Code du Travail)
Action de formation
Effectifs : Min 4 pers. / Max 15 pers.
Calendrier :
1ère et 2ème semaine de décembre 2020
Une session prévue tous les trimestres
Possibilité de sessions sur-mesure

CONTACT

ingenierie-fc@sorbonne-universite.fr

Informations non contractuelles
PDF généré le 26/04/2024

- Analyses statiques de code.
- Propagation de teintes.
- Typage.
- Étude de cas : Linux Security Modules (LSM).
- Sécurisation de code.

MÉTHODES

- Cours théoriques suivis des séances pratiques pour une assimilation parfaite des concepts abordés.
- Méthodes pédagogiques adaptables suivant le niveau et les expériences professionnelles du groupe.
- Equipe pédagogique composée des enseignant–chercheurs et des spécialistes professionnels.
- Supports pédagogiques sous plusieurs formes (papier, électronique, internet,...)
- Évaluation des connaissances acquises.

Documents : Supports de cours PDF

MODALITÉS D'ÉVALUATION

Attestation de fin de formation

ET APRÈS

Cette formation permet aux individus de sécuriser leur parcours professionnel en leur donnant les compétences nécessaires pour accompagner les entreprises dans les enjeux liés à leur secteur d'activité et s'adapter aux évolutions technologiques associées.

LES + DE LA FORMATION

- Une salle cours équipée d'un vidéo-projecteur, d'un tableau numérique, du WiFi et une salle machine de 24 postes de travail avec OS virtualisés sont dédiées à la formation.
- Une plateforme dédiée et un simulateur de cas pratique pour illustrer des attaques internes et externes.

Informations non contractuelles
PDF généré le 26/04/2024