

Parcours métier de Correspondant / Responsable Sécurité Applicative

Référence : SECDEV

Durée : 8 jours

Certification : Aucune

CONNAISSANCES PREALABLES

- Avoir déjà développé ou participé à un projet de développement d'applicatif.
- Avoir suivi le Parcours Introductif Cybersécurité.
- Connaître au moins un langage de développement.
- Connaître le guide d'hygiène sécurité de l'ANSSI.

PROFIL DES STAGIAIRES

- Architectes applicatifs .
- Chefs de projet.
- Concepteurs.
- Développeurs.

OBJECTIFS

- Former les développeurs à la sécurité informatique.
- Transmettre les bonnes pratiques pour intégrer la sécurité informatique dans la conception, le développement et la mise en production.
- Connaître le fonctionnement de la pile.
- Repérer les erreurs dans le code.
- Connaître le rôle des acteurs et la classification des risques : CERT, CWE, OWASP.
- Appliquer les bonnes pratiques.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Module 1

- Les problèmes de sécurité Applicative
- Le monde du WEB : Top 10 OWASP 2017 : Injection - Broken Authentication - Sensitive Data Exposure - XML External Entities - Broken Access Control

Module 2

- Security Misconfiguration
- XSS - CSRF
- Insecure Deserialization
- Vulnérabilités connues
- Manque de supervision et gestion log
- Cycle de développement sécurisé (HTML,PHP,Java (Monde WEB)
- DevOPS

- Recommandation

Module 3

- Le monde Java et la mobilité :
- JVM : Limite de Java - Gestion de la mémoire - Contrôle du bytecode
- Obfuscation : Problématique de la décompilation - Technique d'obfuscation - Hardcodage - Solutions du commerce
- Exécution : Sérialisation des données - Déclaration et initialisation de variable
- Contrôle & Exécution : Contrôle d'accès - Sérialisation des données - Vérification des entrées

Module 4

- Le monde des binaires - C / C++
- Les failles liées aux binaires C/C++
- La gestion mémoire : BufferOverflow - Heap Overflow - String Overflow
- Développement sécurisé : Les chaînes de caractères
- Les pointeurs - Les entiers
- ASLR,DEP,No exec

Module 5

- Vue globale sur les différents langages : Bash - Python - NET
- Pentest : Analyses code source - Fuzzing applicatif - Framework
- La sécurité applicative en mode projet : synthèse

Dates de formation

- Les 9, 10, 26 et 27 Novembre et les 10, 11, 17 et 18 Décembre 2020