EduGroupe
Accompagner pour réussir

Parcours métier de Correspondant / Responsable Sécurité Applicative

Référence : **SECDEV** Durée : **8 jours (56 heures)** Certification : **Aucune**

Connaissances préalables

- 1-Avoir déjà développé ou participé à un projet de développement d'applicatif
- 2-Avoir suivi le Parcours Introductif Cybersécurité
- 3-Connaître au moins un langage de développement
- 4-Connaitre 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 préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

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

Contenu du cours

1. 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

2. 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

3. 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

4. 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

5. 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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.