Mis à jour le 26/07/2023

S'inscrire

Formation SecDevOps : La Sécurité pour le Développement Agile

3 jours (21 heures)

PRÉSENTATION

L'approche SecDevOps met la sécurité des applications comme la plus grande des priorités. C'est pour cela que le terme "Sec" pour sécurité est placé avant le terme "Dev" (signifiant développement) et "Ops" (signifiant opération) en opposition à l'approche DevSecOps où les problématiques de sécurité sont résolues plus tardivement.

Notre formation SecDevOps s'adresse aux développeurs utilisant les méthodes agiles et pratiquant le DevOps. Nous vous enseignerons l'intégration des éléments de sécurité dans les processus Devops afin de réduire les coûts et les délais de réponse suite à une menace cybercriminelle.

Cette formation SecDevOps vous enseignera la culture SecDevOps, la création d'une architecture sécurisée ainsi que sa surveillance. Nous organiserons des études de cas pour mettre ces connaissances en pratique.

OBJECTIFS

- Se familiariser avec les contrôles de sécurité permettant de transformer un processus de développement agile en SecDevOps
- Maîtriser les outils nécessaires pour introduire les tests de sécurité d'une manière automatisée.

PUBLIC VISÉ

- Les équipes de développement qui utilisent des processus agiles en mode DevOps
- Les architectes applicatifs

Pré-requis

Connaissance basique sur la culture DevOps et les processus de développement agiles.

PROGRAMME DE NOTRE FORMATION SecDevOps

Jour 1 : Introduction sur la culture SecDevOps

- Principes et terminologies
- Cycle de développement sécurisé SDLC
- Management de la sécurité dans les processus de développement (ISO 27034)
- OWASP Top 10 et OWASP ASVS
- Tour d'horizon sur les principales vulnérabilités applicatives (SQLi, XSS, CSRF, etc.)

Jour 2 : Conception d'une architecture SecDevOps

- Automatisation des tests de sécurité
- Monitoring de la sécurité
- Intégration de la sécurité dans les workflows des équipes de développement
- L'intelligence artificielle au service de la sécurité/défense proactive
- Analyse et modélisation des risques

Jour 3 : Étude des cas pratiques

- TP 1 : Vue d'ensemble sur la démarche des tests automatisés à l'aide de OWASP ZAP et Jenkins
- TP 2 : Combinaison des outils ZAP, Selenium et Junit pour le scanning des applications
- TP 3 : Utilisation du Framework BDD-Security pour orchestrer les scans automatisés, et intégration dans Jenkins

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.