Développement sécurisé — Secure Coding en Java, Python et JavaScript

Lien : https://innov-systems.com/formation/developpement-securise-secure-coding-en-java-python-et-javascript

DURÉE
5 jours (35h)

RÉFÉRENCE
SI130

CATÉGORIE
Sécurité des Applications

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes du développement sécurisé (Secure Coding)
- Identifier et corriger les vulnérabilités applicatives courantes
- Sécuriser les applications Java, Python et JavaScript
- Mettre en œuvre des mécanismes d’authentification robustes
- Protéger les données sensibles et les secrets applicatifs
- Sécuriser les API web et services backend
- Intégrer la sécurité dans le cycle de développement logiciel
- Appliquer les bonnes pratiques OWASP dans le code
- Réduire les risques d’attaques applicatives
- Mettre en place des tests et audits de sécurité automatisés
- Adopter une approche DevSecOps dans les projets
- Étudier des cas concrets de failles et corrections

POUR QUI ?

- Développeurs Java
- Développeurs Python
- Développeurs JavaScript / Node.js
- Développeurs full-stack
- Architectes logiciels
- DevSecOps engineers
- DevOps engineers
- Consultants en cybersécurité
- Testeurs QA sécurité
- Tech leads
- Toute personne impliquée dans le développement logiciel sécurisé

Innov Systems

Programme détaillé

1 / Introduction au développement sécurisé

- Principes du Secure Coding
- Importance de la sécurité dès le développement
- Panorama des menaces applicatives

2 / Modélisation des risques et menaces

- Identification des surfaces d’attaque
- Threat modeling appliqué aux applications
- Analyse des scénarios d’exploitation

3 / Sécurité en Java

- Gestion sécurisée des entrées utilisateur
- Prévention des injections (SQL, command injection)
- Sécurité des frameworks (Spring Security)

4 / Sécurité en Python

- Validation et sanitation des données
- Sécurisation des APIs Flask/Django
- Gestion sécurisée des dépendances

5 / Sécurité en JavaScript (Frontend & Node.js)

- Prévention des XSS et injections côté client
- Sécurisation des API Node.js
- Gestion sécurisée des tokens JWT

Innov Systems

6 / Authentification et autorisation

- Implémentation sécurisée des sessions
- OAuth2, OpenID Connect et JWT
- Gestion des rôles et permissions

7 / Gestion des données sensibles

- Chiffrement des données sensibles
- Stockage sécurisé des mots de passe (bcrypt, Argon2)
- Protection des secrets applicatifs

8 / Sécurité des APIs

- Sécurisation des endpoints REST et GraphQL
- Rate limiting et anti-abus
- Validation stricte des schémas de données

9 / Tests et audit de sécurité

- SAST et DAST dans le cycle de développement
- Analyse des dépendances (SCA)
- Tests de pénétration applicatifs

10 / Bonnes pratiques et DevSecOps

- Intégration sécurité dans CI/CD
- Secure SDLC et automatisation
- Revue de code sécurisée et standards OWASP

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

18 au 22 Jan. 2027	Présentiel - Casablanca
15 au 19 Mars 2027	Présentiel - Casablanca
10 au 14 Mai 2027	Présentiel - Casablanca
05 au 09 Juil. 2027	Présentiel - Casablanca
30 Août au 03 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés