DAWAN

Plan de la formation

www.dawan.fr

Formation Cybersécurité pour les développeurs : fondamentaux et bonnes pratiques

Durée :	1 jours (7 heures)
Tarifs inter-entreprise :	875,00 € HT (standard) 700,00 € HT (remisé)
Public :	Développeurs juniors
Pré-requis :	Utilisation courante d'un langage de programmation
Objectifs :	Permettre aux développeurs de concevoir, développer et déployer des applications en intégrant les principes essentiels de sécurité, conformément aux attentes actuelles des environnements professionnels.
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102829-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73

Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Introduction à la cybersécurité applicative

Panorama des menaces actuelles ciblant les applications Web et logicielles
Responsabilité du développeur dans la chaîne de sécurité
Principes de sécurité “by design” et “by default”

Vulnérabilités applicatives courantes

Présentation des vulnérabilités les plus fréquentes (OWASP Top 10)
Injections, failles d’authentification, gestion des sessions
Exposition des données sensibles et mauvaises configurations

Atelier pratique
Analyse de cas concrets de failles applicatives
Identification des risques dans un code ou une architecture simple

Bonnes pratiques de développement sécurisé

Gestion sécurisée des mots de passe et des secrets
Validation des entrées et protection contre les injections
Gestion des dépendances et des mises à jour
Journalisation et gestion des erreurs sans fuite d’informations

Sécurité dans les environnements modernes

Sécurisation des API REST
Notions de sécurité côté client et côté serveur
Introduction à la sécurité dans les pipelines CI/CD
Sensibilisation aux risques liés au cloud et aux outils no-code / low-code

Conclusion et mise en perspective

Intégrer la sécurité dans les projets de développement
Bonnes pratiques à maintenir dans le temps
Lien avec les exigences réglementaires (RGPD, protection des données)