

# Abstract formation sécurité

2 jours

Méthodes pédagogiques :  
30% théorique, 70% pratique

Prochaines sessions : retrouvez les dates et le calendrier complet sur notre site [www.arolla.fr/training](http://www.arolla.fr/training)

Offre inter-entreprise : Petit-déjeuner - Déjeuner - Café et collation

## Objectifs :

L'objectif de la formation est de donner les clés pour pouvoir produire une application sécurisée dans un contexte Agile.

Vous pensez que la sécurité, ce n'est pas pour vous? Vous travaillez dans une approche Agile mais respecter les exigences sécurité qui vous sont imposées semble difficile ? Vous savez que la sécurité est importante, mais vous ne savez pas comment la décliner à tous les niveaux de votre projet?

Cette formation est donc faite pour vous !

La sécurité est un sujet exigeant. Suite à cette formation, vous aurez les outils nécessaires pour fournir un produit sûr et utilisable qui réjouira vos clients. Sun Tzu disait : « Connais ton ennemi mieux que toi-même ». C'est pourquoi nous nous mettrons, dans un premier temps, dans la peau d'un attaquant. Puis nous verrons ensuite les solutions possibles pour intégrer la sécurité dans une organisation Agile tout en répondant aux différents parties prenantes de votre projet, que ce soit votre PO ou votre auditeur sécurité.

Durant la formation, nous verrons les thèmes suivants :

- Penser comme un attaquant
- Découvrir les principales attaques Web
- Comprendre le Secure by Design et le Secure Coding
- Décliner la sécurité dans mon organisation et mon projet Agile

A l'issue de cette formation, vous pourrez:

- Avoir une analyse critique sur l'aspect sécurité (organisation, architecture, développement, test & ops)
- Développer de manière sécurisé du code
- Avoir une « boîte à outils sécurité » déclinable dans votre projet

## Programme :

- Connaître les notions fondamentales de la sécurité en matière de logicielle
- Se mettre dans la peau d'un attaquant
- Construire et penser un cycle de vie sécurisée et l'intégrer dans mon organisation Agile
- Du point de vue des développeurs, savoir définir ce qu'il faut prendre en compte pour protéger le système.
- Connaître ses limites, parcours de progression et prendre en compte l'éco-système et le facteur humain dans l'entourage du système
- Concevoir une pipeline de livraison sécurisée et automatiser la sécurité dans votre environnement

## A savoir :

- La formation est donnée en anglais ou en français
- Les supports sont écrits en anglais