

## Formation DevSecOps Foundation (DSOF)

■ <b>Durée :</b>	3 jours (21 heures)
■ <b>Tarifs inter-entreprise :</b>	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
■ <b>Public :</b>	Toute personne impliquée ou intéressée à en savoir plus sur les stratégies et l'automatisation DevSecOps - Toute personne impliquée dans les architectures de chaîne d'outils de livraison continue - à l'équipe de conformité - Directeurs d'entreprise - Personnel de livraison - Ingénieurs DevOps - Directeurs informatiques - Professionnels, praticiens et gestionnaires de la sécurité informatique - Personnel de maintenance et de soutien - Fournisseurs de services gérés - Chefs de projets et de produits - à l'équipes d'assurance qualité - Responsables des versions - Scrum Masters - Ingénieurs en fiabilité des sites - Ingénieurs logiciels - Testeurs
■ <b>Pré-requis :</b>	Une compréhension et une connaissance de la terminologie et des concepts DevOps courants et une expérience de travail connexe sont recommandées.
■ <b>Objectifs :</b>	Comprendre les avantages, les concepts et le vocabulaire de DevSecOps - Différences entre les pratiques de sécurité DevOps et les autres approches de sécurité - Stratégies de sécurité et bonnes pratiques orientées métier - Comprendre et appliquer les données et les sciences de la sécurité - Intégration des parties prenantes de l'entreprise dans les pratiques DevSecOps - Amélioration de la communication entre les équipes Dev, Sec et Ops - Comment les rôles DevSecOps s'inscrivent dans une culture et une organisation DevOps
■ <b>Modalités pédagogiques, techniques et d'encadrement :</b>	<ul style="list-style-type: none"><li>• Formation synchrone en présentiel et distanciel.</li><li>• Méthodologie basée sur l'Active Learning : 75 % de pratique minimum.</li><li>• Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat.</li><li>• Un formateur expert.</li></ul>

<ul style="list-style-type: none"> <li> <b>Modalités d'évaluation :</b> </li> </ul>	<ul style="list-style-type: none"> <li>• Définition des besoins et attentes des apprenants en amont de la formation.</li> <li>• Auto-positionnement à l'entrée et la sortie de la formation.</li> <li>• Suivi continu par les formateurs durant les ateliers pratiques.</li> <li>• Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.</li> </ul>
<ul style="list-style-type: none"> <li> <b>Sanction :</b> </li> </ul>	Attestation de fin de formation mentionnant le résultat des acquis
<ul style="list-style-type: none"> <li> <b>Référence :</b> </li> </ul>	DEV101336-F
<ul style="list-style-type: none"> <li> <b>Note de satisfaction des participants:</b> </li> </ul>	Pas de données disponibles
<ul style="list-style-type: none"> <li> <b>Contacts :</b> </li> </ul>	commercial@dawan.fr - 09 72 37 73 73
<ul style="list-style-type: none"> <li> <b>Modalités d'accès :</b> </li> </ul>	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
<ul style="list-style-type: none"> <li> <b>Délais d'accès :</b> </li> </ul>	Variable selon le type de financement.
<ul style="list-style-type: none"> <li> <b>Accessibilité :</b> </li> </ul>	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

## Réalisation des résultats DevSecOps

Origines du DevOps

Évolution de DevSecOps

CALMES

Les trois voies

## Définition du paysage des cybermenaces

Quel est le paysage des cybermenaces ?

Quelle est la menace ?

De quoi protégeons-nous ?

Que protégeons-nous et pourquoi ?

Comment parler à la sécurité?

## Construire un modèle DevSecOps réactif

Démonstration du modèle  
Résultats techniques, commerciaux et humains  
Que mesure-t-on ?  
Gating et seuillage

## **Intégration des parties prenantes de DevSecOps**

L'état d'esprit DevSecOps  
Les parties prenantes de DevSecOps  
Quels sont les enjeux pour qui?  
Participer au modèle DevSecOps

## **Établissement des meilleures pratiques DevSecOps**

Commencez là où vous êtes  
Intégrer les personnes, les processus et la technologie et la gouvernance  
Modèle d'exploitation DevSecOps  
Pratiques de communication et limites  
Mettre l'accent sur les résultats

## **Bonnes pratiques pour commencer**

Les trois voies  
Identification des états cibles  
Pensée centrée sur la chaîne de valeur

## **Pipelines DevOps et conformité continue**

L'objectif d'un pipeline DevOps  
Pourquoi la conformité continue est importante  
Archétypes et architectures de référence  
Coordination de la construction du pipeline DevOps  
Catégories, types et exemples d'outils DevSecOps

## **Apprendre en utilisant les résultats**

Options de formation à la sécurité  
La formation comme politique  
Apprentissage expérientiel  
Compétences croisées  
Le corpus collectif de connaissances DevSecOps

## **Préparation et passage de la certification**

Qcm de 40 questions

Durée : 60mn

Score minimal à atteindre pour obtenir la certification : 65%