

## Formation Sécuriser un service Docker

■ <b>Durée :</b>	1 jours (7 heures)
■ <b>Tarifs inter-entreprise :</b>	976,00 CHF (standard) 780,80 CHF (remisé)
■ <b>Public :</b>	Administrateurs système/DevOps
■ <b>Pré-requis :</b>	Bonne expérience en matière d'nfrastructure conteneurisée Docker / Bonne connaissance de l'architecture d'un système Linux / Avoir les bases de l'administration d'un système Linux
■ <b>Objectifs :</b>	Connaître les bonnes pratiques et les lignes de défense permettant de sécuriser un service Docker
■ <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>
■ <b>Modalités d'évaluation :</b>	<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>
■ <b>Sanction :</b>	Attestation de fin de formation mentionnant le résultat des acquis
■ <b>Référence :</b>	OUT102385-F
■ <b>Note de satisfaction des participants:</b>	Pas de données disponibles
■ <b>Contacts :</b>	commercial@dawan.fr - 09 72 37 73 73

■ <b>Modalités d'accès :</b>	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
■ <b>Délais d'accès :</b>	Variable selon le type de financement.
■ <b>Accessibilité :</b>	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

## Connaître les bonnes pratiques

Effectuer les mises à jour  
Analyser la sécurité d'une image  
Comprendre les différentes expositions du service Docker  
Éviter de recourir inutilement au compte root : conteneurs rootless  
Mettre en place des limitations de ressources

**Atelier : Mise en œuvre d'une stack Docker avec les bases de la sécurité**

## Identifier les limites des modes avancés

Les risques de partages d'espaces de noms Net et PID  
Le mode privileged et les dangers  
Désactivation des communications inter-conteneurs  
Systèmes de fichiers en lecture seule et exceptions

**Atelier : Amélioration de la sécurité de la stack de l'atelier précédent**

## Mettre en place des lignes de défense

Comprendre les capacités avec Docker  
Sécurité noyau et Docker : AppArmor/SELinux  
Sécurité fine des appels systèmes : Seccomp  
Interdire l'élévation de privilèges : no-new-privileges

**Atelier : Mise en place des lignes de défense avancée (Capability + AppArmor minimal)**

## **Comprendre Docker UserNS**

Principes

Mise en œuvre

Limitations

***Atelier : Configurer le mode UserNS du service Docker***

## **Mettre en œuvre Docker en mode Rootless**

Principes

Mise en œuvre

Limitations

***Atelier : Installation de Docker en mode Rootless***