DAWAN

Plan de la formation

www.dawan.fr

Formation Sécuriser un service Docker

Durée :	1 jours (7 heures)
Tarifs inter-entreprise :	976,00 € HT (standard) 780,80 € HT (remisé)
Public :	Administrateurs système/DevOps
Pré-requis :	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
Objectifs :	Connaître les bonnes pratiques et les lignes de défense permettant de sécuriser un service Docker
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 :	OUT102385-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

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 capabilités 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