DAWAN

Plan de la formation

www.dawan.fr

Formation Sécuriser Docker et Kubernetes

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
Public :	Développeurs, ingénieurs DevOps, administrateurs systèmes / Cloud, architectes techniques
Pré-requis :	Pratique de base de Docker (images, containers) et notions de Kubernetes (pods, services, namespaces)
Objectifs :	Comprendre les risques spécifiques liés aux conteneurs et aux orchestrateurs (Docker, Kubernetes) - Mettre en œuvre les bonnes pratiques de sécurisation des images, registres, nœuds et clusters Kubernetes - Intégrer des contrôles de sécurité dans les pipelines CI/CD autour des conteneurs - Superviser la sécurité des environnements containerisés et limiter l'impact d'une compromission
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 :	CYB102776-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

Comprendre les risques et principes de sécurité des conteneurs

Définir les spécificités de l'architecture conteneurisée par rapport aux VM classiques
Identifier les risques propres aux conteneurs : images non maîtrisées, mauvaises permissions, isolation limitée
Découvrir les bonnes pratiques générales de sécurité Docker et Kubernetes
Relier ces enjeux aux référentiels (CIS Benchmarks, recommandations cloud providers, etc.)
Atelier fil rouge : analyser une architecture containerisée simple et lister les principaux risques potentiels

Sécuriser les images, registres et exécutions Docker

Construire des images durcies : minimiser la surface d'attaque, gérer les dépendances, secrets et utilisateurs
Mettre en place des registres sécurisés : authentification, autorisation, scan de vulnérabilités
Contrôler les options de runtime Docker (capabilities, root, volumes, réseau)
Intégrer les scans d'images dans la chaîne CI/CD pour limiter les vulnérabilités en production
Atelier fil rouge : durcir un Dockerfile existant et définir une politique de scan d'images adaptée

Renforcer la sécurité d'un cluster Kubernetes

Organiser les namespaces, RBAC et comptes de service pour limiter les privilèges
Protéger l'API server, l'accès au cluster et les secrets Kubernetes
Appliquer des politiques réseau (Network Policies) pour limiter les communications entre pods

Utiliser des contrôles d’admission (admission controllers, policies) pour imposer des règles de sécurité
Atelier fil rouge : proposer un modèle de RBAC et de Network Policies pour un cluster Kubernetes d’entreprise

Intégrer la sécurité Kubernetes dans les pipelines et la supervision

Intégrer des scans de configuration (manifests, Helm charts, YAML) dans la CI/CD
Utiliser des outils d’analyse statique de configuration Kubernetes / IaC (Kubernetes, Terraform, etc.)
Centraliser les logs et les événements de sécurité (audit logs, événements cluster, pods)
Mettre en place des alertes sur les comportements anormaux (pods privilégiés, escalades, scans internes)
Atelier fil rouge : définir une chaîne de contrôle de sécurité de la build à la production pour les déploiements Kubernetes

Limiter l’impact d’une compromission et améliorer en continu

Concevoir des architectures résilientes et cloisonnées pour limiter la propagation d’une attaque
Planifier les mises à jour (cluster, nœuds, images) et la gestion des vulnérabilités
Mettre en place une démarche d’audit régulier (benchmarks, revues de configuration, revues d’images)
Élaborer une feuille de route d’amélioration continue pour la sécurité des conteneurs et clusters
Atelier fil rouge final : construire un plan de durcissement par étapes d’un contexte Docker / Kubernetes existant