DAWAN

Plan de la formation

www.dawan.fr

Formation DevSecOps : sécuriser la chaîne CI/CD et l’Infrastructure as Code

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
Public :	Développeurs, ingénieurs DevOps, SRE, architectes, responsables sécurité travaillant avec des équipes DevOps
Pré-requis :	Connaissance pratique d’au moins un outil de CI/CD (GitLab CI, GitHub Actions, Jenkins…) et notions de Cloud / conteneurs
Objectifs :	Comprendre les principes du DevSecOps et du « shift-left » en sécurité - Intégrer des contrôles de sécurité dans la chaîne CI/CD (code, dépendances, images, configuration) - Sécuriser l’Infrastructure as Code (IaC) et les configurations d’environnements Cloud / containerisés - Mettre en place une démarche outillée et progressive pour industrialiser la sécurité dans les pipelines
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 :	CYB102777-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 principes du DevSecOps et du shift-left

Définir DevSecOps et ses différences avec les approches DevOps classiques
Comprendre le concept de « shift-left » et l'intégration de la sécurité tout au long du cycle de vie
Identifier les acteurs impliqués : Dev, Ops, Sec, Produit, Métiers
Cartographier une chaîne CI/CD type et repérer les points d'injection possibles de contrôles de sécurité
Atelier fil rouge : représenter la chaîne CI/CD de son organisation ou d'un cas d'école et identifier les points de contrôle potentiels

Intégrer la sécurité dans la chaîne CI/CD

Mettre en place des contrôles sur le code source : scan SAST, secrets, dépendances (SCA)
Sécuriser les images conteneurs dans les pipelines (scan d'images, réputation, politiques d'acceptation)
Contrôler la qualité des tests (tests de sécurité automatisés, fuzzing, tests API)
Gérer les résultats de scans et prioriser les corrections pour ne pas bloquer la livraison en continu
Atelier fil rouge : enrichir un pipeline CI/CD existant avec des étapes de scan de code, dépendances et images

Sécuriser l'Infrastructure as Code (IaC)

Identifier les principaux outils IaC (Terraform, Ansible, CloudFormation, Helm, etc.)
Comprendre les risques liés à l'IaC (mauvaises configurations répliquées, secrets dans les fichiers, sur-exposition réseau)

Mettre en œuvre des scans de configuration et des policies “as code” sur l’IaC
Intégrer ces contrôles dans les pipelines de build et de déploiement
Atelier fil rouge : analyser des fichiers Terraform / YAML et corriger des faiblesses de sécurité identifiées

Industrialiser DevSecOps : politiques, outils et collaboration

Définir des politiques de sécurité adaptées au contexte DevOps (niveau de sévérité, seuils de blocage)
Sélectionner et intégrer les outils adaptés à l’écosystème (SAST, SCA, DAST, IaC scan, secrets detection, etc.)
Organiser la collaboration entre équipes : revue conjointe des priorités, gestion des exceptions, backlog sécurité
Suivre des indicateurs de performance DevSecOps (vulnérabilités ouvertes, temps de correction, couverture scans)
Atelier fil rouge : construire un modèle de gouvernance DevSecOps et un tableau de bord de suivi des risques dans les pipelines

Construire une feuille de route DevSecOps réaliste

Évaluer la maturité actuelle de l’organisation en matière de DevSecOps
Identifier les quick wins et les chantiers structurants à plus long terme
Planifier le déploiement progressif des contrôles et des outils sur les différents projets et équipes
Préparer l’accompagnement au changement (formation, documentation, coaching) pour les équipes Dev et Ops
Atelier fil rouge final : formaliser une feuille de route DevSecOps sur 6 à 18 mois pour son contexte ou un cas d’école