+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 25/04/2025

S'inscrire

Formation DevSecOps - Intégrer la Sécurité au Cœur du DevOps

1 jour (7 heures)

PRÉSENTATION

Notre formation DevSecOps offre aux architectes, développeurs et experts sécurité une vision partagée des enjeux, leur permettant de parler le même langage et d'initier une démarche structurée.

Notre programme de formation s'adresse aux professionnels du développement, de l'infrastructure ou de la sécurité souhaitant intégrer des pratiques DevSecOps concrètes dans leurs projets.

Des démonstrations et des retours d'expérience viendront illustrer comment une culture SecOps solide permet aux architectes, développeurs et équipes de sécurité de parler le même langage et collaborer de manière fluide.

À l'issue de cette formation, vous aurez une vue claire sur les possibilités offertes par le SecOps dans votre entreprise.

OBJECTIFS

- Comprendre les concepts fondamentaux du DevSecOps
- Détecter et prévenir les vulnérabilités (code, dépendances, conteneurs, secrets…)
- Mettre en œuvre une chaîne CI/CD sécurisée
- Maîtriser les outils clés comme Bandit, Trivy, Checkov, KubeLinter, Syft et NeuVector

PUBLIC VISÉ

- Architectes logiciels
- Équipe Cybersécurité
- Développeurs référents

- Éventuellement, Ops/Administrateurs système intéressés par l’aspect sécurité

Prérequis

- Bonne compréhension des pratiques DevOps et CI/CD
- Bases en développement
- Connaissances de base en Docker et Infrastructure as Code (Terraform, Kubernetes)
- Accés Internet sans restrictions (VPN, proxy, etc.) pour accéder aux environnements des TPs

Programme de notre formation DevSecOps

Introduction au DevSecOps

- Qu'est-ce que DevSecOps ?
- L'évolution du DevSecOps
- L'importance de la sécurité dans le SDLC
- L'approche "Shift Left"
- Le rôle de l'automatisation dans DevSecOps
- Les bénéfices de DevSecOps

Git, IaC, Infrastructure Immuable et GitOps

- Considérations générales sur la sécurité Git
- Comment l'infrastructure immuable améliore la sécurité
- Élimination des drifts de configuration
- GitOps : le futur de la gestion d'infrastructure

Gestion et Prévention des Secrets

- Le problème croissant de la prolifération des secrets
- Les niveaux de fuite de secrets
- Hooks pré-commit
- TP : Prévenir les fuites de secrets avec TruffleHog

Dépendances Sécurisées

- La menace croissante des attaques via les dépendances
- Vulnérabilités et expositions communes (CVEs)
- Système de notation des vulnérabilités (CVSS)
- Énumération des faiblesses communes (CWE)
- Énumération des plateformes communes (CPE)
- TP : OWASP Dependency-Check

Qualité et Sécurité du Code

- L'importance de la qualité et de la sécurité du code
- Comprendre les arbres syntaxiques abstraits (ASTs)
- Pièges courants de sécurité dans le code
- TP : Bandit - linter de sécurité Python

Sécurité des Conteneurs

- Dockerfile : linting de sécurité
- Sécuriser les Dockerfiles
- Pièges de sécurité courants dans les Dockerfiles
- TP : Hadolint - exemple pratique de linting
- Linting Dockerfile vs scan d'image Docker
- TP : Scanner les images Docker avec Trivy
- Comprendre les rapports Trivy

Collaboration Sécurisée avec IaC (Terraform)

- Gestion des secrets
- Contrôle d'accès basé sur les rôles (RBAC) et principe du moindre privilège
- Stockage distant de l'état
- Atténuation du drift et conformité

Analyse de Code IaC

- Pièges de sécurité courants dans l'IaC (Terraform)
- Sécurité Terraform avec Checkov
- Problèmes de sécurité fréquents dans les manifestes Kubernetes
- TP : Analyse statique avec KubeLinter

Chaîne d'Approvisionnement Logicielle et SBOM

- Importance de la sécurité de la chaîne d'approvisionnement
- Comprendre les SBOMs (Software Bill of Materials)
- Rôle des SBOMs dans DevSecOps
- TP : Utiliser Syft pour l'analyse
- TP : Syft et OWASP DependencyTrack

Politique de Sécurité comme Code (SPaC)

- SAST, DAST, et approche Shift Left
- Conformité et audit
- Pare-feu d'applications web (WAF)
- Capteurs de prévention des pertes de données (DLP)
- Règles de réponse et gestion des incidents
- TP : NeuVector - exemple pratique de SPaC

Pipeline DevSecOps

- DevSecOps comme système
- CI/CD comme colonne vertébrale
- Construire un pipeline DevSecOps (GitLab CI/CD)

Mesurer et Améliorer DevSecOps

- Boucles de rétroaction, couverture, métriques et sécurité
- Apprendre des échecs
- Shift Left, étendre à droite
- Indicateurs de succès (KPIs)

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.