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

Mis à jour le 10/09/2025

S'inscrire

Formation Digital.AI Release

3 jours (21 heures)

Présentation

Notre formation vous présente Digital.ai Release, une plateforme d'orchestration DevSecOps qui centralise et automatise la gestion des workflows de livraison logicielle. Conçue pour des environnements hybrides et multi-cloud, elle permet de standardiser les déploiements, d'automatiser les validations et tests de conformité, et de garantir une traçabilité complète des processus de delivery.

Cette formation Digital.ai Release vous permettra de maîtriser la mise en œuvre de workflows complexes intégrant tests automatisés, contrôles de sécurité et validations multi-équipes. Vous découvrirez comment renforcer la qualité de vos releases grâce à l'automatisation des scénarios de tests, à l'intégration d'outils de supervision et à l'industrialisation des rapports d'audit.

Grâce à des ateliers pratiques, vous apprendrez à modéliser et sécuriser vos pipelines, à intégrer des tests fonctionnels, de sécurité et de performance directement dans vos workflows, et à superviser vos environnements à grande échelle.

Vous serez également capables de connecter Release à vos outils d'automatisation existants (Jenkins, GitHub/GitLab, Terraform, Ansible, plateformes de test) pour créer une chaîne DevSecOps robuste et pilotée par la qualité.

À l'issue de la formation, vous serez en mesure de mettre en place une chaîne DevSecOps automatisée, d'industrialiser vos stratégies de test et de conformité, et de piloter vos releases dans un cadre sécurisé et gouverné.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable de Digital.AI Release.

Objectifs

- Comprendre les fondamentaux de Digital.ai Release
- Orchestrer des pipelines DevSecOps sécurisés et audités
- Automatiser la conformité (rapports, contrôles, traçabilité)
- Intégrer Release à l’écosystème CI/CD & cloud
- Mettre en place des KPI et optimiser la Value Stream

Public visé

- Ingénieurs DevOps
- Équipes sécurité IT
- Tech leads

Pré-requis

- Expérience de base en cloud et/ou IaC

Programme de notre formation Digital.ai Release

[Jour 1 - Matin]

Vue d’ensemble de Digital.ai Release

- Positionnement de Digital.ai Release dans un écosystème DevSecOps
- Concepts clés : orchestration, gouvernance, traçabilité, audits
- Architecture : serveur Release, workers, plugins, API
- Panorama des intégrations (Jenkins, GitHub Actions, GitLab, Terraform)
- Stratégies de modélisation des workflows et bonnes pratiques
- Atelier pratique : Installation et configuration initiale.

[Jour 1 - Après-midi]

Modéliser des pipelines sécurisés

- Conception de pipelines multi-environnements
- Gates d’approbation, RBAC et contrôles qualité
- Gestion centralisée des clés et secrets via Vault
- Politique de versioning et traçabilité des artefacts
- Patterns d’idempotence et de reprise
- Atelier pratique : Pipeline sécurisé avec validations.

Conformité & audit by design

- Exigences RGPD, SOX, HIPAA : principes et cartographie
- Journalisation : activités, changements, approbations, écarts
- Génération automatisée de rapports d’audit
- Politiques réutilisables et templates d’organisation
- Gestion des risques et matrices de contrôles
- Atelier pratique : Pipeline avec rapport de conformité.

[Jour 2 - Matin]

CI/CD : connecter l’écosystème

- Connecteurs Jenkins, GitHub Actions, GitLab CI : triggers & feedback
- Webhooks, Git triggers, conditions et paramètres dynamiques
- Gestion des artefacts (registries, repositories, SBOM)
- Notifications (mail, Slack, Teams)
- Stratégies de rollback et blue-green/canary
- Atelier pratique : Orchestrer un job Jenkins depuis Release.

[Jour 2 - Après-midi]

Infrastructure as Code & cloud

- Provisioning Terraform/Ansible depuis Release
- Orchestration hybride entre environnements locaux et cloud
- Gestion de la drift et remédiations automatiques
- Kubernetes & Operators : installation/upgrade pilotés
- Sécurisation des comptes cloud et least privilege
- Atelier pratique : Stack IaC multi-comptes avec validations.

Qualité, sécurité applicative & SCA

- Intégrer SAST/DAST et Software Composition Analysis
- Politiques de gate sécurité (scores, CVSS, licences)
- Tests et qualimétrie dans le pipeline
- Centralisation via tableau de bord Release
- Automatiser les remédiations et exceptions
- Atelier pratique : Gate sécurité avec SCA.

[Jour 3 - Matin]

Supervision & optimisation continue

- Métriques & KPI (DORA, temps de cycle, CFR)
- Gestion des incidents, retries, timeouts
- Observabilité : intégrations Prometheus/Grafana/SIEM

- Optimisation des workers et parallélisations
- Maîtrise des coûts & efficience
- Atelier pratique : Suivi des indicateurs et gestion proactive des incidents.

[Jour 3 - Après-midi]

Gouvernance & multi-équipes/produits

- Modèles réutilisables & bibliothèques d’étapes
- Multi-tenancy, permissions, cloisonnement
- Gestion des fenêtres de release et freezes
- Stratégies de migration/upgrade et EOL plugins
- Bonnes pratiques d’exploitation & support
- Atelier pratique : Création d’une bibliothèque de templates pour industrialiser les pipelines.

Étude de cas & rétro-planification

- Cartographier un flux valeur bout-en-bout
- Définir la routemap d’industrialisation DevSecOps
- Construire un plan de conformité auditable
- Mesurer l’impact (qualité, sécurité, coûts)
- Préparer la généralisation & l’acculturation
- Atelier pratique : Préparation des livrables et plan de mise en production.

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.