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

Updated on 12/09/2025

Sign up

Digital.AI Release Training

3 days (21 hours)

Presentation

Our training course introduces you to Digital.ai Release, a DevSecOps orchestration platform that centralizes and automates the management of software delivery workflows. Designed for hybrid and multi-cloud environments, it standardizes deployments, automates validation and compliance testing, and guarantees complete traceability of delivery processes.

This Digital.ai Release training course will enable you to master the implementation of complex workflows integrating automated tests, security checks and multi-team validations. You'll discover how to enhance the quality of your releases by automating test scenarios, integrating supervision tools and industrializing audit reports.

Through hands-on workshops, you'll learn how to model and secure your pipelines, integrate functional, security and performance tests directly into your workflows, and supervise your large-scale environments.

You'll also be able to connect Release to your existing automation tools (Jenkins, GitHub/GitLab, Terraform, Ansible, testing platforms) to create a robust, quality-driven DevSecOps chain.

At the end of the course, you'll be able to set up an automated DevSecOps chain, industrialize your testing and compliance strategies, and manage your releases within a secure, governed framework.

Like all our training courses, this one is based on the latest stable version of Digital.AI Release.

Objectives

- Understand the fundamentals of Digital.ai Release
- Orchestrate secure and audited DevSecOps pipelines
- Automate compliance (reporting, controls, traceability)
- Integrate Release into the CI/CD & cloud ecosystem
- Set up KPIs and optimize Value Stream

Target audience

- DevOps engineers
- IT security teams
- Tech leads

Prerequisites

- Basic experience in cloud and/or IaC

Our Digital.ai Release training program

[Day 1 - Morning]

Overview of Digital.ai Release

- Positioning Digital.ai Release in a DevSecOps ecosystem
- Key concepts: orchestration, governance, traceability, audits
- Architecture: Release server, workers, plugins, APIs
- Overview of integrations (Jenkins, GitHub Actions, GitLab, Terraform)
- Workflow modeling strategies and best practices
- Practical workshop: Installation and initial configuration.

[Day 1 - Afternoon]

Modeling secure pipelines

- Multi-environment pipeline design
- Approval gates, RBAC and quality control
- Centralized key and secret management via Vault
- Versioning policy and artifact traceability
- Idempotency and recovery patterns
- Practical workshop: Secure pipeline with validations.

Compliance & audit by design

- RGPD, SOX, HIPAA requirements: principles and mapping
- Logging: activities, changes, approvals, deviations
- Automated generation of audit reports
- Reusable policies and organizational templates
- Risk management and control matrices
- Practical workshop: Pipeline with compliance report.

[Day 2 - Morning]

CI/CD: connecting the ecosystem

- Jenkins connectors, GitHub Actions, GitLab CI: triggers & feedback
- Webhooks, Git triggers, conditions and dynamic parameters
- Artifact management (registries, repositories, SBOM)
- Notifications (mail, Slack, Teams)
- Rollback and blue-green/canary strategies
- Practical workshop: Orchestrating a Jenkins job from Release.

[Day 2 - Afternoon] Infrastructure

as Code & cloud

- Terraform/Ansible provisioning from Release
- Hybrid orchestration between local and cloud environments
- Drift management and automatic remediation
- Kubernetes & Operators: controlled installation/upgrade
- Securing cloud accounts and least privilege
- Practical workshop: Multi-account IaC stack with validations.

Quality, application security & SCA

- Integrating SAST/DAST and Software Composition Analysis
- Gate security policies (scores, CVSS, licenses)
- Pipeline testing and qualimetry
- Centralization via Release dashboard
- Automating remediation and exceptions
- Practical workshop: Gate security with SCA.

[Day 3 - Morning]

Supervision & continuous optimization

- Metrics & KPIs (DORA, cycle time, CFR)
- Incident management, retries, timeouts
- Observability: Prometheus/Grafana/SIEM integrations

- Worker optimization and parallelization
- Cost control & efficiency
- Practical workshop: Indicator monitoring and proactive incident management.

[Day 3 - Afternoon]

Governance & multi-teams/products

- Reusable templates & step libraries
- Multi-tenancy, permissions, partitioning
- Managing release windows and freezes
- Migration/upgrade strategies and EOL plugins
- Good operating practices & support
- Practical workshop: Creating a template library to industrialize pipelines.

Case study & reverse planning

- Mapping an end-to-end value stream
- Defining the DevSecOps industrialization roadmap
- Build an auditable compliance plan
- Measure impact (quality, security, costs)
- Prepare for generalization & acculturation
- Practical workshop: Preparation of deliverables and production launch plan.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming training course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples and

and group work sessions.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire training course.