



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

DevSecOps & Secure Software Supply Chain Specialist

Course + certificate

On request

VAT excluded

Course code

DEVSECOPS-PIPELINE

Minimum duration

456 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Advanced pathway for developers, security engineers, architects and platform teams that must integrate security, compliance and governance into software development and release pipelines.

This extended technical dossier describes the pathway as published in CIWZ Academy on the issue date. It consolidates purpose, references, learning architecture, module contents, assessment system, passing criteria and certificate conditions. It does not replace the official texts of the standards, laws, guidelines or schemes referenced.

2. Normative, regulatory and technical references

NIST SP 800-218 SSDF; OWASP SAMM; OWASP ASVS; SLSA; software supply-chain security best practices; CI/CD security guidance

References are used as the learning and assessment framework within the limits of published content and available sources. For professional application, the official and current versions of the referenced documents always prevail.

3. Learning architecture and assessment system

- 8 structured learning modules
- minimum tracked time: 456 min
- intermediate-check bank: 256 questions
- active final-exam bank: 240 questions
- final exam: 30 questions selected from the bank
- passing threshold: 75%
- Access to the pathway through the personal Academy profile or a corporate assignment.
- Sequential study of the modules, with server-side recording of progress and required minimum time.

- Intermediate checks linked to modules to verify understanding, application capability and quality of reasoning.
- Final exam unlock only after the pathway requirements have been completed.
- Protected final exam assembled by the platform through selection from the active course question bank.
- Recording of the result and, where applicable, the option to request the final certificate.

4. Official catalogue technical information

Course technical sheet

Specialist CIWZ Academy pathway with original content, server-tracked lessons, 8 modules, randomized intermediate checks, protected final assessment and a scenario-based question bank. Indicative average market benchmark: EUR 1,890 (typical range EUR 1,290 – EUR 2,690). Free access; any fee applies only to certificate issuance after passing.

5. Detailed course syllabus

The following syllabus is derived from the active modules published on the platform. Each module shows its minimum study time and the size of its available intermediate-check bank.

01 DevSecOps model, roles and operational targets

Minimum time: 57 min | Intermediate questions: 32

02 Secure coding, threat modeling and security requirements

Minimum time: 57 min | Intermediate questions: 32

03 CI/CD hardening and pipeline secrets

Minimum time: 57 min | Intermediate questions: 32

04 SAST, SCA, secret scanning and quality gates

Minimum time: 57 min | Intermediate questions: 32

05 Containers, artifacts and supply-chain trust

Minimum time: 57 min | Intermediate questions: 32

06 Dynamic testing, API security and release assurance

Minimum time: 57 min | Intermediate questions: 32

07 Policy-as-code, IaC and secure environments

Minimum time: 57 min | Intermediate questions: 32

08 Metrics, operating model and continuous improvement

Minimum time: 57 min | Intermediate questions: 32

6. Developed module-by-module contents

The following pages analytically describe the content actually associated with each platform module. The structure is designed so that learners, companies, HR, Quality, HSE or CISO functions can understand precisely what is studied and assessed.

MODULE 01**DevSecOps model, roles and operational targets**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Turn security from a final gate into a distributed responsibility across planning, coding, build, test, release and operations.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define roles, policies, scorecards, readiness criteria and escalation for security defects.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Define roles, policies, scorecards, readiness criteria and escalation for security defects.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: RACI, SDLC policy, quality gates, release criteria and secure-backlog evidence.

Professional scenario

The team releases often but security intervenes only at sprint end: redesign the flow. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Lead time for security fixes and percentage of releases meeting gates.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Security as a bottleneck, theoretical policies, no owners for findings.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "DevSecOps model, roles and operational targets".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 02**Secure coding, threat modeling and security requirements**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Translate business and risk requirements into user stories, misuse cases, abuse cases and development controls.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply practical threat modeling, secure design review and mitigation patterns.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Apply practical threat modeling, secure design review and mitigation patterns.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Threat models, abuse cases, secure architecture reviews and security acceptance criteria.

Professional scenario

A new API is designed without authentication and rate limiting requirements: close the gap before release. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Threat-model coverage and recurring vulnerabilities by error family.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Threat modeling performed once, implicit requirements, merely formal reviews.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Secure coding, threat modeling and security requirements".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 03**CI/CD hardening and pipeline secrets**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Protect repositories, runners, artifacts, secrets and approvals in the release pipeline.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Segment runners, handle signing, OIDC workload identity, secret vaults and branch protection.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Segment runners, handle signing, OIDC workload identity, secret vaults and branch protection.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Evidence of pipeline configuration, approvals, secret inventory, signing status and branch policies.

Professional scenario

A shared runner can read secrets from multiple projects: define an isolated and verifiable model. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Signing coverage, hardcoded secrets detected, percentage of protected pipelines.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Secrets in CI, privileged runners, branches without mandatory review.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "CI/CD hardening and pipeline secrets".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 04**SAST, SCA, secret scanning and quality gates**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Integrate automated controls into builds sustainably, distinguishing severity, exploitability and context.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use SAST, SCA, IaC scanning, secret scanning and gating policies calibrated to the application and criticality.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use SAST, SCA, IaC scanning, secret scanning and gating policies calibrated to the application and criticality.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Scan reports, waiver registers, quality-gate history and false-positive tuning notes.

Professional scenario

Pipelines produce thousands of findings and the team ignores them: define priorities and governance. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: False-positive rate, critical-finding MTTR, percentage of correctly blocked builds.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Alert overload, no prioritization, unreviewed exceptions, inconsistent gating.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "SAST, SCA, secret scanning and quality gates".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 05**Containers, artifacts and supply-chain trust**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Ensure integrity and provenance of images, packages and dependencies across the software supply chain.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply SBOMs, provenance, artifact signing, repository trust and dependency governance.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Apply SBOMs, provenance, artifact signing, repository trust and dependency governance.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: SBOMs, signed artifacts, dependency policies, repository-mirror evidence and provenance logs.

Professional scenario

A compromised dependency reaches production through a transitive dependency: design the defenses. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: SBOM coverage, signed-artifact ratio, reaction time to critical CVEs.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: No build reproducibility, dependencies without owners, unverified provenance.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Containers, artifacts and supply-chain trust".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 06**Dynamic testing, API security and release assurance**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Integrate DAST, API testing, targeted fuzzing and pre-release assurance pragmatically.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Link dynamic testing to threat models, use cases and the most likely abuse scenarios.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Link dynamic testing to threat models, use cases and the most likely abuse scenarios.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: DAST/API reports, release sign-off, test evidence and remediation backlog.

Professional scenario

The application passes the build but fails authorization controls in staging: handle the release. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Defects found pre-release vs post-release and critical-API test coverage.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Generic dynamic testing, unmapped APIs, releases validated only by functional behaviour.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Dynamic testing, API security and release assurance".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 07**Policy-as-code, IaC and secure environments**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Make infrastructure verifiable through code, policy and drift control across the lifecycle.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Manage baselines, change review, environment parity and drift remediation.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Manage baselines, change review, environment parity and drift remediation.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: IaC repositories, policy packs, drift reports, environment approvals and exception records.

Professional scenario

A manual production change bypasses IaC and controls: restore governance of change. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Resources outside IaC, open drift, recurring policy-violation rate.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: ClickOps, outdated templates, policy-as-code not enforced.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Policy-as-code, IaC and secure environments".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 08**Metrics, operating model and continuous improvement**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Measure DevSecOps-program effectiveness so it remains sustainable and truly adopted.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use metrics that drive decisions: exposure, fix lead time, waiver quality and release confidence.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use metrics that drive decisions: exposure, fix lead time, waiver quality and release confidence.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Quarterly scorecards, operating reviews, risk acceptance and training evidence.

Professional scenario

Management asks for speed without seeing accumulated security debt: build useful dashboards. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Fix lead time, backlog aging, exemption quality and escaped defects.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Cosmetic KPIs, inconsistent data, improvement not tied to decisions.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Metrics, operating model and continuous improvement".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

7. Assessment system, final exam and passing criteria

- Intermediate checks are linked to individual modules and provide progressive learning control before access to the final assessment.
- The final assessment consists of 30 questions selected from the active course bank. The platform applies an anti-repetition logic for new attempts when the bank size allows it.
- Final question-bank size detected at generation time: 240 active questions.
- Published passing threshold for the course: 75%.
- Questions are intended to assess not only recall but also interpretation, application, evidence selection, scenario assessment and quality of decision-making, depending on the subject matter.

8. Tracking, learning continuity and session integrity

- Path status, completed modules and recorded time are managed server-side when the course uses the Academy learning mode.
- The platform allows the pathway to resume from the recorded point and retains the results of required checks.
- Assessment sessions may be subject to the integrity and proctoring controls enabled by the platform and described in the applicable usage rules.
- Technical and integrity events support assessment and do not replace professional judgement where human review is required.

9. Certificate, use and limitations

The CIWZ certificate, where provided by the pathway and requested after passing, records the result achieved in the stated CIWZ pathway or assessment. It does not automatically replace personnel certification, professional registration, statutory licence, legal qualification or credentials issued by third-party bodies where such requirements are imposed by the applicable scheme.

10. Commercial and tax conditions

- Course + certificate: On request VAT excluded.
- UAE VAT is applied to UAE customers according to billing data and the applicable tax rules.
- Any specific commercial terms, agreements or corporate orders override the public price only when formally accepted by Certificato IWZ FZCO.

11. Dossier document control

- Document automatically generated by CIWZ Academy from the course data published at the time of the request.

- Course code: DEVSECOPS-PIPELINE
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.