



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Kubernetes & Container Security Specialist

Course + certificate

On request

VAT excluded

Course code

K8S-CONTAINER-SEC

Minimum duration

424 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Advanced pathway for cloud-native operators focused on container security, Kubernetes orchestration, admission control, runtime, networking and software supply chain.

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 800-190; CIS Kubernetes Benchmark; NSA/CISA Kubernetes guidance; container supply-chain best practices

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: 424 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 1,790 (typical range EUR 1,190 – EUR 2,490). 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 Kubernetes architecture and attack surface

Minimum time: 53 min | Intermediate questions: 32

02 Image security, registry and provenance

Minimum time: 53 min | Intermediate questions: 32

03 RBAC, service accounts and access control

Minimum time: 53 min | Intermediate questions: 32

04 Pod security, admission control and policy

Minimum time: 53 min | Intermediate questions: 32

05 Network policies, service mesh and east-west communications

Minimum time: 53 min | Intermediate questions: 32

06 Secrets, configuration and persistent data

Minimum time: 53 min | Intermediate questions: 32

07 Runtime security, eBPF and incident response

Minimum time: 53 min | Intermediate questions: 32

08 Cluster operations, upgrade and continuous assurance

Minimum time: 53 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**Kubernetes architecture and attack surface**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Understand control-plane, worker-node, add-on components and cluster trust boundaries.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Map attack surfaces of API server, kubelet, etcd, ingress, CNI and storage.

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: Map attack surfaces of API server, kubelet, etcd, ingress, CNI and storage.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Cluster diagrams, component inventory and configuration baselines.

Professional scenario

The cluster grows without formal design: identify the highest-risk areas. 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: Number of unmanaged components and control-plane exposure.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Exposed control plane, uninventoried components, ad hoc addons.

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 "Kubernetes architecture and attack surface".

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**Image security, registry and provenance**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Defend the lifecycle of container images from build to runtime.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use image signing, scanning, base-image governance and registry trust.

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 image signing, scanning, base-image governance and registry trust.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: SBOMs, image scans, signing status, pull policies and registry access logs.

Professional scenario

A custom image is manually updated on a node: restore control. 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: Signed-image coverage, open critical CVEs, base-image age.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Unsigned images, uncontrolled public registries, latest tags in production.

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 "Image security, registry and provenance".

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**RBAC, service accounts and access control**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Apply least privilege to users, service accounts, operators and workloads.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Limit cluster-admin permissions, token exposure and impersonation.

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: Limit cluster-admin permissions, token exposure and impersonation.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: RBAC matrices, service-account inventory, audit logs and access-review evidence.

Professional scenario

An application namespace uses cluster-wide privileges for convenience: correct the 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: Privileged accounts, non-rotated tokens, overdue RBAC reviews.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Wildcard roles, reused service accounts, shared kubeconfigs.

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 "RBAC, service accounts and access control".

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**Pod security, admission control and policy**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Reduce workload privileges and prevent dangerous configurations.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use Pod Security Standards, admission policies, OPA/Kyverno and secure defaults.

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 Pod Security Standards, admission policies, OPA/Kyverno and secure defaults.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Policy reports, denied-admission logs, namespace baselines and exception registers.

Professional scenario

A team requests privileged containers in production: assess alternatives and exceptions. 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: Compliant pods, open exceptions, meaningful admission-deny rate.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Uncontrolled HostPath, runAsRoot, policies bypassed via special namespaces.

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 "Pod security, admission control and policy".

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**Network policies, service mesh and east-west communications**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Control intra-cluster and outbound traffic through segmentation and identity-aware networking.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define default-deny, ingress/egress policies, mTLS and traffic observability.

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 default-deny, ingress/egress policies, mTLS and traffic observability.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Network-policy inventory, mesh configuration, flow logs and exposure mapping.

Professional scenario

A compromised pod can laterally reach critical services: contain the impact. 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: Namespaces with default deny, mTLS coverage, unnecessarily exposed services.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Flat networking, wildcard ingress, open egress, unmonitored DNS abuse.

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 "Network policies, service mesh and east-west communications".

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**Secrets, configuration and persistent data**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Protect secrets, config maps, volumes and persistent data connected to the cluster.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use secret stores, encryption at rest, CSI drivers, rotation and secure storage classes.

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 secret stores, encryption at rest, CSI drivers, rotation and secure storage classes.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Secret-store config, encryption status, storage policies and PV inventory.

Professional scenario

Credentials are distributed as unrotated environment variables: correct the design. 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: Secrets outside vaults, unencrypted volumes, average secret age.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Secrets in YAML, sensitive config maps, volumes with undefined retention.

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 "Secrets, configuration and persistent data".

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**Runtime security, eBPF and incident response**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Detect anomalous activity and respond in containerized environments without losing evidence.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Configure runtime monitoring, process/network policies and forensic collection.

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: Configure runtime monitoring, process/network policies and forensic collection.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Runtime alerts, incident playbooks, node-isolation procedures and evidence-collection notes.

Professional scenario

A container downloads unexpected binaries at runtime: handle containment and analysis. 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: Runtime MTTD, confirmed alerts, containment of compromised workloads.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Noisy alerts, no runbooks, stopping the whole cluster as the only response.

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 "Runtime security, eBPF and incident response".

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**Cluster operations, upgrade and continuous assurance**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Sustain cluster security over time across upgrades, new services and changing workloads.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Integrate scanning, benchmark review, drift control, upgrade testing and dashboards.

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: Integrate scanning, benchmark review, drift control, upgrade testing and dashboards.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Benchmark reports, upgrade plans, drift reports and operational-review evidence.

Professional scenario

A platform upgrade risks nullifying existing security policies: plan the 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: Clusters meeting benchmarks, open drift, out-of-support versions.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Untested upgrades, snowflake configurations, security treated as sporadic ticketing.

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 "Cluster operations, upgrade and continuous 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.

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: K8S-CONTAINER-SEC
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.