



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

Kubernetes & Container Security Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

K8S-CONTAINER-SEC

Durata minima

424 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso avanzato per operatori cloud-native dedicato a sicurezza dei container, orchestrazione Kubernetes, admission control, runtime, networking e supply chain.

La presente scheda tecnica estesa descrive il percorso così come pubblicato nella CIWZ Academy alla data di emissione. Riunisce finalità, riferimenti, architettura didattica, contenuti dei moduli, sistema delle verifiche, criteri di superamento e condizioni di attestazione. Il documento non sostituisce i testi ufficiali delle norme, delle leggi, delle linee guida o degli schemi richiamati.

2. Riferimenti normativi, regolamentari e tecnici

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

I riferimenti sono utilizzati come quadro di studio e di valutazione nei limiti del contenuto pubblicato e delle fonti disponibili. Per l'applicazione professionale prevalgono sempre le versioni ufficiali e vigenti dei documenti richiamati.

3. Architettura didattica e sistema di verifica

- 8 moduli didattici strutturati
- tempo minimo tracciato: 424 min
- banca verifiche intermedie: 256 quesiti
- banca esame finale attiva: 240 quesiti
- esame finale: 30 quesiti selezionati dalla banca
- soglia di superamento: 75%
- Accesso al percorso attraverso il profilo Academy personale o tramite assegnazione aziendale.
- Studio sequenziale dei moduli, con registrazione server-side dell'avanzamento e del tempo minimo previsto.

- Verifiche intermedie associate ai moduli per controllare comprensione, capacità applicativa e qualità del ragionamento.
- Sblocco dell'esame finale solo dopo il completamento dei requisiti previsti dal percorso.
- Esame finale protetto, composto dalla piattaforma mediante selezione dalla banca attiva del corso.
- Registrazione dell'esito e, quando previsto, possibilità di richiedere l'attestato finale.

4. Informazioni tecniche ufficiali di catalogo

Scheda tecnica del corso

Percorso CIWZ Academy specialistico e operativo con contenuti originali, lezioni tracciate lato server, 8 moduli, verifiche intermedie randomizzate, assessment finale protetto e banca domande scenario-based. Benchmark medio di mercato indicativo: € 1.790 (range tipico € 1.190 – € 2.490). Accesso gratuito; eventuale costo solo per l'emissione del certificato dopo il superamento.

5. Programma analitico del percorso

Il programma seguente è ricavato dai moduli attivi pubblicati nella piattaforma. Per ciascun modulo sono indicati il tempo minimo e la consistenza della banca di verifica intermedia disponibile.

01 Architettura Kubernetes e superficie d'attacco

Tempo minimo: 53 min | Quesiti intermedi: 32

02 Image security, registry e provenienza

Tempo minimo: 53 min | Quesiti intermedi: 32

03 RBAC, service account e controllo accessi

Tempo minimo: 53 min | Quesiti intermedi: 32

04 Pod security, admission control e policy

Tempo minimo: 53 min | Quesiti intermedi: 32

05 Network policies, service mesh e comunicazioni est-ovest

Tempo minimo: 53 min | Quesiti intermedi: 32

06 Secrets, configurazioni e dati persistenti

Tempo minimo: 53 min | Quesiti intermedi: 32

07 Runtime security, eBPF e risposta agli incidenti

Tempo minimo: 53 min | Quesiti intermedi: 32

08 Cluster operations, upgrade e continuous assurance

Tempo minimo: 53 min | Quesiti intermedi: 32

6. Contenuti sviluppati modulo per modulo

Le pagine seguenti descrivono in modo analitico i contenuti effettivamente associati a ciascun modulo della piattaforma. La struttura è concepita per consentire a candidato, azienda, HR, Quality, HSE o CISO di comprendere con precisione cosa viene studiato e verificato.

MODULO 01**Architettura Kubernetes e superficie d'attacco**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Comprendere componenti control plane, worker node, add-on e trust boundary del cluster.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Mappare superficie d'attacco di API server, kubelet, etcd, ingress, CNI e storage.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Mappare superficie d'attacco di API server, kubelet, etcd, ingress, CNI e storage.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Diagrammi cluster, inventory componenti, configuration baseline.

Scenario professionale

Il cluster cresce senza design formale: identificare le aree di maggior rischio. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Numero di componenti non gestiti e exposure del control plane.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Control plane accessibile, componenti non inventariati, addon installati ad hoc.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Architettura Kubernetes e superficie d'attacco".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 02**Image security, registry e provenienza**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Difendere il ciclo di vita delle immagini container dalla build al runtime.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare image signing, scan, base image governance e registry trust.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Usare image signing, scan, base image governance e registry trust.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: SBOM, image scan, signing status, pull policy, registry access logs.

Scenario professionale

Una image custom viene aggiornata manualmente su un nodo: ripristinare il controllo. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Coverage image signed, CVE critiche aperte, base image age.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Image non firmate, registries pubblici senza controllo, tag latest in produzione.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Image security, registry e provenienza".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 03**RBAC, service account e controllo accessi**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Applicare least privilege a utenti, service account, operator e workload.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Limitare permessi cluster-admin, token exposure e impersonation.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Limitare permessi cluster-admin, token exposure e impersonation.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: RBAC matrix, service-account inventory, audit logs, access-review evidence.

Scenario professionale

Un namespace applicativo usa permessi cluster-wide per comodità: correggere il modello. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Account privilegiati, token non ruotati, review RBAC scadute.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Ruoli wildcard, service account riutilizzati, kubeconfig condivisi.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "RBAC, service account e controllo accessi".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 04**Pod security, admission control e policy**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Ridurre i privilegi dei workload e prevenire configurazioni pericolose.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare Pod Security Standards, admission policy, OPA/Kyverno e default secure.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Usare Pod Security Standards, admission policy, OPA/Kyverno e default secure.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Policy report, denied admission logs, namespace baseline, exception register.

Scenario professionale

Un team richiede privileged containers in produzione: valutare alternative e deroghe. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Pod compliant, eccezioni aperte, admission deny rate significativo.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: HostPath non governato, runAsRoot, policy bypassate con namespace speciali.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Pod security, admission control e policy".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 05**Network policies, service mesh e comunicazioni est-ovest**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Controllare il traffico intra-cluster e verso l'esterno con segmentazione e identity-aware networking.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire default deny, ingress/egress policy, mTLS e osservabilità del traffico.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Definire default deny, ingress/egress policy, mTLS e osservabilità del traffico.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Network policy inventory, mesh config, flow logs, exposure mapping.

Scenario professionale

Un pod compromesso può raggiungere lateralmente servizi critici: contenere l'impatto. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Namespaces con default deny, copertura mTLS, servizi esposti inutilmente.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Flat networking, ingress wildcard, egress aperto, DNS abuse non monitorato.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Network policies, service mesh e comunicazioni est-ovest".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 06**Secrets, configurazioni e dati persistenti**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Proteggere secret, configmap, volumi e dati persistenti collegati al cluster.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare secret store, encryption at rest, CSI driver, rotation e storage class sicure.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Usare secret store, encryption at rest, CSI driver, rotation e storage class sicure.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Secret-store config, encryption status, storage policy, PV inventory.

Scenario professionale

Le credenziali sono distribuite come environment variable non ruotate: correggere il design. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Segreti fuori vault, volumi non cifrati, età media dei secret.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Secret in YAML, configmap sensibili, volumi con retention non definita.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Secrets, configurazioni e dati persistenti".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 07**Runtime security, eBPF e risposta agli incidenti**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Rilevare attività anomale e rispondere in ambienti containerizzati senza perdere evidenze.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Configurare runtime monitoring, process/network policies e collection forense.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Configurare runtime monitoring, process/network policies e collection forense.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Runtime alerts, incident playbook, node isolation procedure, evidence collection notes.

Scenario professionale

Un container scarica binari imprevisti in runtime: gestire containment e analisi. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: MTTD runtime, alert confermati, contenimento workload compromessi.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Alert rumorosi, no runbook, arresto del cluster come unica risposta.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Runtime security, eBPF e risposta agli incidenti".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

MODULO 08**Cluster operations, upgrade e continuous assurance**

- Tempo minimo previsto: 53 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Mantenere nel tempo il livello di sicurezza del cluster tra upgrade, nuovi servizi e changing workloads.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Integrare scanning, benchmark review, drift control, upgrade testing e dashboard.

Metodo operativo

Applicare il seguente schema: definire obiettivo e rischio, progettare la misura, implementarla in modo controllato, raccogliere evidenze, misurarne l'efficacia e riesaminarla. In questo modulo: Integrare scanning, benchmark review, drift control, upgrade testing e dashboard.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Benchmark reports, upgrade plan, drift report, operational review evidence.

Scenario professionale

L'upgrade della piattaforma rischia di annullare policy di sicurezza esistenti: pianificare il change. L'analisi deve distinguere urgenza, rischio residuo, owner, compensazioni e criteri di accettazione.

KPI, KRI e segnali deboli

Misurare non solo l'implementazione ma anche l'efficacia. Indicatori minimi: Cluster con benchmark conforme, drift aperto, versioni fuori supporto.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Upgrade senza test, configurazioni snowflake, sicurezza trattata come ticket sporadico.

Laboratorio decisionale

Esercizio: un cambiamento, un'anomalia o una richiesta di business impongono di scegliere rapidamente. Descrivere la decisione, i criteri, le evidenze da raccogliere e il test di efficacia. Applicarlo al tema "Cluster operations, upgrade e continuous assurance".

Preparazione alla verifica

Prima del test finale, verifica di saper spiegare il perché di una scelta tecnica, identificare almeno due alternative, indicare le evidenze necessarie e motivare quale configurazione è realmente sostenibile.

7. Sistema di verifica, esame finale e criteri di superamento

- Le verifiche intermedie sono collegate ai singoli moduli e costituiscono un controllo progressivo dell'apprendimento prima dell'accesso alla prova finale.
- La prova finale è composta da 30 quesiti selezionati dalla banca attiva del corso. La piattaforma applica una logica anti-ripetizione per i nuovi tentativi quando la consistenza della banca lo consente.
- Consistenza della banca finale rilevata al momento della generazione: 240 quesiti attivi.
- Soglia di superamento pubblicata per il corso: 75%.
- Le domande sono finalizzate a verificare non soltanto il richiamo mnemonico, ma anche interpretazione, applicazione, selezione delle evidenze, valutazione di scenari e qualità della decisione, in funzione della materia trattata.

8. Tracciamento, continuità didattica e integrità della sessione

- Lo stato del percorso, i moduli completati e il tempo registrato sono gestiti lato server quando il corso utilizza la modalità formativa Academy.
- La piattaforma consente la ripresa del percorso dal punto registrato e conserva gli esiti delle verifiche previste.
- Le sessioni di verifica possono essere soggette ai controlli di integrità e proctoring attivati dalla piattaforma e descritti nelle regole di utilizzo applicabili.
- Gli eventi tecnici e di integrità sono elementi di supporto alla valutazione e non sostituiscono il giudizio professionale quando è prevista una revisione umana.

9. Attestazione, utilizzo e limiti del documento

L'attestato CIWZ, quando previsto dal percorso e richiesto dopo il superamento, documenta il risultato ottenuto nel percorso o nella prova CIWZ indicata. Non sostituisce automaticamente certificazioni di persona, iscrizioni ad albi, abilitazioni professionali, qualifiche legali o credenziali rilasciate da organismi o soggetti terzi quando tali requisiti sono previsti dallo schema applicabile.

10. Condizioni economiche e fiscali

- Corso + attestato: Su richiesta IVA/VAT esclusa.
- La UAE VAT viene applicata ai clienti UAE secondo i dati di fatturazione e la normativa fiscale applicabile.
- Eventuali condizioni commerciali specifiche, convenzioni o ordini aziendali prevalgono sul prezzo pubblico solo se formalmente accettati da Certificato IWZ FZCO.

11. Controllo documentale della scheda

- Documento generato automaticamente dalla CIWZ Academy sulla base dei dati del corso pubblicati al momento della richiesta.
- Codice corso: K8S-CONTAINER-SEC
- Lingua documento: IT
- Data di generazione: 13/10/2026
- Per l'applicazione normativa e professionale fanno fede le fonti ufficiali vigenti e le eventuali procedure/schema applicabili.