



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

DevSecOps & Secure Software Supply Chain Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

DEVSECOPS-PIPELINE

Durata minima

456 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso avanzato per sviluppatori, security engineer, architect e platform team che devono integrare sicurezza, compliance e governance nella catena di sviluppo e rilascio del software.

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

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: 456 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: € 1.890 (range tipico € 1.290 – € 2.690). 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 Modello DevSecOps, ruoli e target operativi

Tempo minimo: 57 min | Quesiti intermedi: 32

02 Secure coding, threat modeling e requisiti di sicurezza

Tempo minimo: 57 min | Quesiti intermedi: 32

03 CI/CD hardening e segreti di pipeline

Tempo minimo: 57 min | Quesiti intermedi: 32

04 SAST, SCA, secret scanning e quality gates

Tempo minimo: 57 min | Quesiti intermedi: 32

05 Container, artefatti e supply chain trust

Tempo minimo: 57 min | Quesiti intermedi: 32

06 Security testing dinamico, API e release assurance

Tempo minimo: 57 min | Quesiti intermedi: 32

07 Policy-as-code, IaC e ambienti sicuri

Tempo minimo: 57 min | Quesiti intermedi: 32

08 Metriche, operating model e continuous improvement

Tempo minimo: 57 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**Modello DevSecOps, ruoli e target operativi**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Trasformare la sicurezza da gate finale a responsabilità distribuita lungo planning, coding, build, test, release e operations.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire ruoli, policy, scorecard, readiness criteria e escalation per difetti di sicurezza.

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 ruoli, policy, scorecard, readiness criteria e escalation per difetti di sicurezza.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: RACI, policy SDLC, quality gate, release criteria, secure backlog evidence.

Scenario professionale

Il team rilascia spesso ma la sicurezza interviene solo a fine sprint: ridisegnare il flusso. 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: Lead time per fix sicurezza e percentuale release conformi ai gate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Security come collo di bottiglia, policy teoriche, assenza di owner per le findings.

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 "Modello DevSecOps, ruoli e target operativi".

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**Secure coding, threat modeling e requisiti di sicurezza**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Tradurre requisiti di business e di rischio in user story, misuse case, abuse case e controlli di sviluppo.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare threat modeling pratico, secure design review e pattern di mitigazione.

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: Applicare threat modeling pratico, secure design review e pattern di mitigazione.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Threat model, abuse cases, secure architecture review, security acceptance criteria.

Scenario professionale

Una nuova API nasce senza requisiti di autenticazione e rate limiting: colmare il gap prima del rilascio. 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: Copertura threat model e vulnerabilità ricorrenti per famiglia di errore.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Threat model fatto una sola volta, requisiti impliciti, review solo formale.

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 "Secure coding, threat modeling e requisiti di sicurezza".

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**CI/CD hardening e segreti di pipeline**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Proteggere repository, runner, artifact, secret e approvazioni nella pipeline di rilascio.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Segmentare runner, gestire signing, OIDC workload identity, secret vault e branch protection.

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: Segmentare runner, gestire signing, OIDC workload identity, secret vault e branch protection.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Evidence di pipeline config, approvals, secret inventory, signing status e branch policy.

Scenario professionale

Un runner condiviso può leggere segreti di più progetti: definire un modello isolato e verificabile. 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: Copertura signing, segreti hardcoded rilevati, percentuale pipeline con protection.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Segreti nel CI, runner privileged, branch senza review obbligatoria.

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 "CI/CD hardening e segreti di pipeline".

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**SAST, SCA, secret scanning e quality gates**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Integrare controlli automatici nel build in modo sostenibile, distinguendo severità, exploitability e contesto.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare SAST, SCA, IaC scan, secret scan e policy di gating calibrate per applicazione e criticità.

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 SAST, SCA, IaC scan, secret scan e policy di gating calibrate per applicazione e criticità.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Scan reports, waiver register, quality-gate history, false-positive tuning notes.

Scenario professionale

Le pipeline producono migliaia di findings e il team le ignora: definire priorità e governance. 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: False-positive rate, MTTR findings critiche, percentuale build bloccate correttamente.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Allarme totale, nessuna priorità, eccezioni non riesaminate, gating incoerente.

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 "SAST, SCA, secret scanning e quality gates".

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**Container, artefatti e supply chain trust**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Garantire integrità e provenienza di immagini, pacchetti e dipendenze lungo la supply chain software.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare SBOM, provenance, artifact signing, repository trust e dependency governance.

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: Applicare SBOM, provenance, artifact signing, repository trust e dependency governance.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: SBOM, signed artifacts, dependency policy, repository mirror evidence, provenance logs.

Scenario professionale

Una dipendenza compromessa entra in produzione tramite transitive dependency: progettare le difese. 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: SBOM coverage, signed artifacts ratio, tempo di reazione a CVE critiche.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Build riproducibilità assente, dipendenze senza owner, provenance non verificata.

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 "Container, artefatti e supply chain trust".

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**Security testing dinamico, API e release assurance**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Integrare DAST, API testing, fuzzing mirato e pre-release assurance in modo pragmatico.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Collegare test dinamici a threat model, use case e scenari di abuso più probabili.

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: Collegare test dinamici a threat model, use case e scenari di abuso più probabili.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: DAST/API reports, release sign-off, test evidence, remediation backlog.

Scenario professionale

L'applicazione supera il build ma fallisce sui controlli di autorizzazione in staging: gestire il rilascio. 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: Difetti rilevati pre-release vs post-release e coverage test API critiche.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Testing dinamico generico, API non mappate, release validate solo dal funzionamento.

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 "Security testing dinamico, API e release 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.

MODULO 07**Policy-as-code, IaC e ambienti sicuri**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Rendere verificabile l'infrastruttura tramite codice, policy e drift control lungo tutto il ciclo.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Gestire baseline, change review, environment parity e remediation del drift.

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: Gestire baseline, change review, environment parity e remediation del drift.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: IaC repositories, policy packs, drift reports, environment approvals, exception records.

Scenario professionale

Una modifica manuale in produzione aggira IaC e controlli: ripristinare il governo del cambiamento. 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: Risorse fuori IaC, drift aperto, policy violation recurring rate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: ClickOps, template obsoleti, policy-as-code non enforce.

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 "Policy-as-code, IaC e ambienti sicuri".

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**Metriche, operating model e continuous improvement**

- Tempo minimo previsto: 57 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Misurare efficacia del programma DevSecOps per renderlo sostenibile e realmente adottato.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare metriche che guidano decisioni: exposure, fix lead time, waiver quality, release confidence.

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 metriche che guidano decisioni: exposure, fix lead time, waiver quality, release confidence.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Scorecard trimestrali, operating review, risk acceptance, training evidence.

Scenario professionale

Il management chiede velocità senza vedere il debito di sicurezza accumulato: costruire dashboard utili. 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: Fix lead time, backlog aging, exemption quality, escaped defects.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: KPI cosmetici, dati incoerenti, miglioramento non collegato a decisioni.

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 "Metriche, operating model e continuous improvement".

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: DEVSECOPS-PIPELINE
- 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.