



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

OT / ICS / IIoT Cybersecurity Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

OT-ICS-SEC

Durata minima

480 min

Soglia finale

75%

Edizione scheda

14/10/2026

1. Identità, finalità e perimetro del percorso

Percorso specialistico per proteggere ambienti industriali, OT e sistemi di controllo con approccio asset-driven, sicuro e compatibile con la continuità di processo.

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

IEC 62443 family; NIST SP 800-82 Rev.3; MITRE ATT&CK for ICS; industrial network security 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: 480 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: € 2.790 (range tipico € 1.890 – € 3.990). 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 Contesto OT/ICS, safety e processo

Tempo minimo: 60 min | Quesiti intermedi: 32

02 Architetture Purdue, segmentazione e accesso remoto

Tempo minimo: 60 min | Quesiti intermedi: 32

03 Asset visibility, protocol awareness e monitoring passivo

Tempo minimo: 60 min | Quesiti intermedi: 32

04 Hardening di PLC, HMI, workstation e server OT

Tempo minimo: 60 min | Quesiti intermedi: 32

05 Identity, accessi privilegiati e change control OT

Tempo minimo: 60 min | Quesiti intermedi: 32

06 Detection, incident response e recovery in OT

Tempo minimo: 60 min | Quesiti intermedi: 32

07 IIoT, edge e integrazione IT/OT

Tempo minimo: 60 min | Quesiti intermedi: 32

08 Governance, programma 62443 e maturità operativa

Tempo minimo: 60 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**Contesto OT/ICS, safety e processo**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Comprendere la differenza tra IT e OT, le priorità safety/availability e le peculiarità dei sistemi industriali.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Mappare processo, asset, zone, conduits e impatti su sicurezza fisica e continuità.

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 processo, asset, zone, conduits e impatti su sicurezza fisica e continuità.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Asset inventory, process map, zone/conduit model, criticality matrix.

Scenario professionale

Uno stabilimento modernizza linee ma non conosce tutti gli asset OT: avviare la discovery sicura. 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 asset OT e zone con owner definito.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: OT trattata come IT, assenza di process view, asset invisibili.

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 "Contesto OT/ICS, safety e processo".

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**Architetture Purdue, segmentazione e accesso remoto**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Progettare reti industriali segmentate e accessi remoti sicuri senza compromettere il processo.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare zone/conduits, jump host, remote vendor control, firewall industriali e monitoring.

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 zone/conduits, jump host, remote vendor control, firewall industriali e monitoring.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Network architecture, remote-access procedure, firewall rules, vendor access logs.

Scenario professionale

Un fornitore mantiene PLC con VPN permanente: ridisegnare l'accesso. 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: Sessioni remote controllate, segmentazione implementata, eccezioni aperte.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Flat plant network, accessi permanenti, dual-homed device non governati.

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 "Architetture Purdue, segmentazione e accesso remoto".

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**Asset visibility, protocol awareness e monitoring passivo**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Ottenere visibilità su protocolli industriali, baseline e anomalie senza interrompere il processo.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare discovery passiva, protocol decoders, asset fingerprinting e baseline comportamentali.

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 discovery passiva, protocol decoders, asset fingerprinting e baseline comportamentali.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Passive-monitor inventory, protocol map, baseline anomalies, traffic reports.

Scenario professionale

Una cella usa protocolli legacy non documentati: costruire la baseline operativa. 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: Asset individuati, protocolli decodificati, anomalie confermate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Scan attivi non autorizzati, protocolli sconosciuti, baseline assente.

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 "Asset visibility, protocol awareness e monitoring passivo".

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**Hardening di PLC, HMI, workstation e server OT**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Applicare misure di hardening compatibili con vendor support e disponibilità di impianto.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Gestire account, application control, patching controllato, removable media e service minimization.

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 account, application control, patching controllato, removable media e service minimization.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Hardening baseline, vendor matrix, patch approval, workstation control evidence.

Scenario professionale

Un HMI critico non può essere patchato nel breve: definire compensazioni efficaci. 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: Stazioni conformi alla baseline, patch overdue, removable media exceptions.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Patch indiscriminate o assente, account locali condivisi, USB senza regole.

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 "Hardening di PLC, HMI, workstation e server OT".

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**Identity, accessi privilegiati e change control OT**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Mettere sotto controllo accessi, modifiche e responsabilità negli ambienti OT.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Separare ruoli, gestire credenziali shared vendor, logging di modifica e approvazioni.

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: Separare ruoli, gestire credenziali shared vendor, logging di modifica e approvazioni.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Access register, change tickets, configuration backups, approval evidence.

Scenario professionale

Una modifica PLC d'emergenza viene fatta senza tracciabilità: ricostruire il processo. 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: Change con approvazione, backup configurazione, accessi privilegiati riesaminati.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Credenziali condivise inevitabili ma non governate, change control bypassato.

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 "Identity, accessi privilegiati e change control OT".

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**Detection, incident response e recovery in OT**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Preparare risposta e ripristino per eventi OT con impatto su sicurezza fisica e continuità.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire trigger, ruoli, decisioni di isolamento, raccolta evidenze e recovery sicuro.

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 trigger, ruoli, decisioni di isolamento, raccolta evidenze e recovery sicuro.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: OT incident playbook, escalation map, recovery procedure, evidence checklist.

Scenario professionale

Una stazione engineering è sospetta ma lo shutdown del processo è rischioso: decidere la risposta. 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: Tempo di rilevazione, incidenti con playbook adeguato, esiti di recovery test.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: IR solo IT-centric, recovery non testato, decisioni improvvisate.

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 "Detection, incident response e recovery in OT".

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**IIoT, edge e integrazione IT/OT**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Gestire sensori, gateway, edge platform e interconnessione tra OT, cloud e analytics.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Valutare trust boundary, autenticazione, aggiornamenti, remote management e data flow.

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: Valutare trust boundary, autenticazione, aggiornamenti, remote management e data flow.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: IIoT architecture, data-flow map, edge security baseline, device inventory.

Scenario professionale

Nuovi sensori IIoT vengono collegati alla rete impianto senza standard: introdurre 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: Device governati, aggiornamenti sicuri, flussi dati autorizzati.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Shadow IIoT, gateway non gestiti, trust boundary confusa.

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 "IIoT, edge e integrazione IT/OT".

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**Governance, programma 62443 e maturità operativa**

- Tempo minimo previsto: 60 min
- Banca di verifica intermedia disponibile: 32 quesiti

Executive briefing

Portare la sicurezza OT a livello di programma continuativo, misurabile e sostenibile.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Tradurre 62443 in roadmap, ruoli, requisiti minimi e metriche di maturità.

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: Tradurre 62443 in roadmap, ruoli, requisiti minimi e metriche di maturità.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Roadmap OT, maturity assessment, policy set, governance minutes.

Scenario professionale

La direzione investe solo dopo gli incidenti: costruire un programma credibile. 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: Maturity trend, asset coverage, open risks, progress on roadmap.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Iniziative isolate, requisiti generici copiati dall'IT, governance intermittente.

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 "Governance, programma 62443 e maturità operativa".

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: OT-ICS-SEC
- Lingua documento: IT
- Data di generazione: 14/10/2026
- Per l'applicazione normativa e professionale fanno fede le fonti ufficiali vigenti e le eventuali procedure/schema applicabili.