



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

SOC Engineering, SIEM & Detection Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

SOC-DETECTION-ENG

Durata minima

456 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso tecnico per progettare use case, fonti dati, regole di correlazione, pipeline di telemetry e modelli operativi SOC realmente utilizzabili.

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

MITRE ATT&CK; detection engineering best practices; Sigma; OpenTelemetry; SOC operating model 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: € 2.090 (range tipico € 1.390 – € 2.890). 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 Missione del SOC e modello operativo

Tempo minimo: 57 min | Quesiti intermedi: 32

02 Telemetry architecture e data onboarding

Tempo minimo: 57 min | Quesiti intermedi: 32

03 Use case design e detection-as-code

Tempo minimo: 57 min | Quesiti intermedi: 32

04 Correlation, enrichment e prioritizzazione

Tempo minimo: 57 min | Quesiti intermedi: 32

05 Detection validation, purple teaming e coverage review

Tempo minimo: 57 min | Quesiti intermedi: 32

06 Triage, investigation e case management

Tempo minimo: 57 min | Quesiti intermedi: 32

07 SOAR, automazione e controllo del rischio operativo

Tempo minimo: 57 min | Quesiti intermedi: 32

08 Reporting, continuous improvement e SOC economics

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**Missione del SOC e modello operativo**

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

Executive briefing

Definire il ruolo del SOC, i confini con IT, incident response, threat intel e gestione vulnerabilità.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Stabilire service model, tiering, ownership e KPI orientati alla detection efficace.

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: Stabilire service model, tiering, ownership e KPI orientati alla detection efficace.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Operating model, escalation matrix, KPI/SLA, use-case governance.

Scenario professionale

Il SOC riceve ogni allarme senza priorità di business: reimpostare 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: Alert rilevanti gestiti nei tempi, backlog ad alta severità, qualità triage.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: SOC senza mandato chiaro, ownership frammentato, KPI di sola quantità.

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 "Missione del SOC e modello operativo".

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**Telemetry architecture e data onboarding**

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

Executive briefing

Costruire un'architettura dati affidabile per raccogliere, normalizzare e arricchire eventi di sicurezza.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Selezionare fonti prioritarie, parser, schema comuni, enrichments e data quality checks.

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: Selezionare fonti prioritarie, parser, schema comuni, enrichments e data quality checks.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Data-source inventory, parser mapping, field completeness, onboarding checklist.

Scenario professionale

I log esistono ma non sono interrogabili in modo coerente: correggere la pipeline dati. 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 fonti critiche, perdita eventi, completezza campi chiave.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Onboarding senza priorità, campi incoerenti, ingestion cost fuori controllo.

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 "Telemetry architecture e data onboarding".

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**Use case design e detection-as-code**

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

Executive briefing

Tradurre minacce, abuso e casi reali in regole di rilevazione mantenibili.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare ATT&CK, Sigma, hypothesis-driven design e versionamento delle detection.

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 ATT&CK, Sigma, hypothesis-driven design e versionamento delle detection.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Detection catalog, rule logic, ATT&CK mapping, version history, tuning notes.

Scenario professionale

Una regola utile genera troppo rumore: ottimizzare senza perdere copertura. 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: Precisione detection, tasso falsi positivi, coverage ATT&CK dei top risks.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Regole duplicate, naming caotico, detection non versionate.

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 "Use case design e detection-as-code".

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**Correlation, enrichment e prioritizzazione**

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

Executive briefing

Aumentare il valore del SIEM correlando eventi, identità, asset, contesto e intelligence.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire scoring, suppression, enrichment con CMDB/EDR/IAM e business criticality.

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 scoring, suppression, enrichment con CMDB/EDR/IAM e business criticality.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Enrichment map, scoring matrix, suppression logic, context dictionary.

Scenario professionale

Gli analisti vedono alert tecnici ma non sanno quali asset sono critici: chiudere il gap. 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: Alert con contesto business, escalation corrette, riduzione noise rate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Correlazioni casuali, threat intel usata senza validazione, priority drift.

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 "Correlation, enrichment e prioritizzazione".

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**Detection validation, purple teaming e coverage review**

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

Executive briefing

Verificare che le detection funzionino davvero con test controllati e review periodiche.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare emulazione ATT&CK, purple teaming, validation dataset e review post-incident.

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 emulazione ATT&CK, purple teaming, validation dataset e review post-incident.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Test plan, validation results, simulation logs, detection gap register.

Scenario professionale

Una detection esiste da mesi ma nessuno ha verificato se scatta: introdurre assurance. 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: Percentuale detection validate, gap chiusi, coverage per top scenario.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Regole mai testate, coverage presunta, miglioramento solo reattivo.

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 validation, purple teaming e coverage review".

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**Triage, investigation e case management**

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

Executive briefing

Standardizzare triage, pivot di analisi, handoff e raccolta evidenze tra livelli SOC.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Definire runbook, severity model, hypothesis discipline e decision logging.

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 runbook, severity model, hypothesis discipline e decision logging.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Runbook, case template, evidence checklist, investigation notes.

Scenario professionale

Due analisti gestiscono lo stesso alert in modo opposto: normalizzare 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: MTTA, percentuale casi con evidenze complete, riaperture di ticket.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Case management debole, note povere, severità variabile per analista.

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 "Triage, investigation e case management".

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**SOAR, automazione e controllo del rischio operativo**

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

Executive briefing

Automatizzare dove conviene senza aumentare il rischio di azioni sbagliate.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare human-in-the-loop, safe actions, rollback e metriche di efficacia dell'automazione.

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 human-in-the-loop, safe actions, rollback e metriche di efficacia dell'automazione.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Playbook SOAR, approval flow, execution logs, rollback evidence.

Scenario professionale

Una playbook disabilita automaticamente account critici creando danni operativi: 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: Run automatici riusciti, rollback, riduzione tempi triage.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Automazione cieca, playbook senza owner, assenza di test e rollback.

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 "SOAR, automazione e controllo del rischio operativo".

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**Reporting, continuous improvement e SOC economics**

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

Executive briefing

Dimostrare il valore del SOC con reporting leggibile e miglioramento misurabile.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Bilanciare copertura, tempi, qualità, costo e rischio residuo con dashboard direzionali.

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: Bilanciare copertura, tempi, qualità, costo e rischio residuo con dashboard direzionali.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Executive dashboard, cost model, improvement roadmap, governance minutes.

Scenario professionale

Il board vede solo numero ticket e non capisce l'efficacia del SOC: ricostruire il reporting. 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/MTTR, top gap detection, cost per use case, coverage trend.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Reporting tecnico incomprensibile, assenza di priorità, costi non collegati al risultato.

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 "Reporting, continuous improvement e SOC economics".

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: SOC-DETECTION-ENG
- 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.