



DOSSIER TECNICO DIDATTICO E DI VALUTAZIONE

Threat Hunting & Detection Engineering Specialist

Corso + attestato

Su richiesta

IVA/VAT esclusa

Codice corso

THREAT-HUNTING

Durata minima

424 min

Soglia finale

75%

Edizione scheda

13/10/2026

1. Identità, finalità e perimetro del percorso

Percorso specialistico per professionisti che vogliono condurre threat hunting strutturato, hypothesis-driven detection engineering e analisi di indicatori, comportamenti e anomalie.

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; Pyramid of Pain; YARA; Sigma; hunting tradecraft 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: € 1.950 (range tipico € 1.290 – € 2.790). 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 Mentalità di threat hunting e definizione delle ipotesi

Tempo minimo: 53 min | Quesiti intermedi: 32

02 Data preparation, pivot e arricchimento

Tempo minimo: 53 min | Quesiti intermedi: 32

03 Behaviour analytics e ATT&CK-based hunting

Tempo minimo: 53 min | Quesiti intermedi: 32

04 YARA, Sigma e contenuti di detection

Tempo minimo: 53 min | Quesiti intermedi: 32

05 Endpoint, identity e lateral movement hunting

Tempo minimo: 53 min | Quesiti intermedi: 32

06 Cloud e SaaS hunting

Tempo minimo: 53 min | Quesiti intermedi: 32

07 Reporting tecnico e trasformazione in detection

Tempo minimo: 53 min | Quesiti intermedi: 32

08 Programma continuo, skill e governance

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**Mentalità di threat hunting e definizione delle ipotesi**

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

Executive briefing

Passare da caccia casuale a hunting guidato da ipotesi, dati e priorità di rischio.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Generare ipotesi a partire da minacce, asset, exposure e intelligence affidabile.

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: Generare ipotesi a partire da minacce, asset, exposure e intelligence affidabile.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Hunting charter, priority matrix, hypothesis backlog, target scope.

Scenario professionale

Il team "fa hunting" ma senza scopo preciso: introdurre metodo e priorità. 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: Ipotesi validate, cicli chiusi, percentuale hunt collegati a top risk.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Caccia opportunistica, obiettivi vaghi, risultati non riusabili.

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 "Mentalità di threat hunting e definizione delle ipotesi".

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**Data preparation, pivot e arricchimento**

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

Executive briefing

Preparare i dati giusti per muoversi velocemente tra endpoint, rete, identità e cloud.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare pivot, timeline, enrichment e query patterns ripetibili.

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 pivot, timeline, enrichment e query patterns ripetibili.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Data dictionary, pivot playbook, query library, entity mappings.

Scenario professionale

Una potenziale catena d'attacco richiede dati da fonti scollegate: costruire i collegamenti. 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 medio per pivot significativo e copertura delle fonti utili.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Dati non allineati, timestamp incoerenti, entità non normalizzate.

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 "Data preparation, pivot e arricchimento".

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**Behaviour analytics e ATT&CK-based hunting**

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

Executive briefing

Cercare comportamenti ostili più che singoli IOC, collegandoli a tattiche e tecniche.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Applicare query basate su ATT&CK, chain di comportamento e baseline deviations.

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 query basate su ATT&CK, chain di comportamento e baseline deviations.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: ATT&CK coverage map, hunt queries, behaviour library, baseline evidence.

Scenario professionale

Gli IOC storici non producono risultati ma il rischio resta alto: spostarsi sul behaviour hunting. 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 top techniques, hit ratio, hunts trasformati in detection.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: IOC-only mindset, hunting scollegato dagli scenari di minaccia.

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 "Behaviour analytics e ATT&CK-based hunting".

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**YARA, Sigma e contenuti di detection**

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

Executive briefing

Sviluppare contenuti riutilizzabili per memory, file, log e comportamento.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Creare e mantenere regole YARA/Sigma coerenti con hunt e detection pipeline.

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: Creare e mantenere regole YARA/Sigma coerenti con hunt e detection pipeline.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Rule repository, version history, validation notes, false-positive analysis.

Scenario professionale

Una regola è utile in laboratorio ma impraticabile in produzione: renderla sostenibile. 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: Rule precision, deployment success, ratio hunt-to-detection.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Contenuti non versionati, tuning assente, regole non validate.

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 "YARA, Sigma e contenuti di detection".

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**Endpoint, identity e lateral movement hunting**

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

Executive briefing

Riconoscere pattern di compromissione endpoint e movimenti laterali tra identità e sistemi.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Usare process tree, auth events, privilege changes, admin tools e session trail.

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 process tree, auth events, privilege changes, admin tools e session trail.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Process evidence, auth pivots, account behaviour analysis, lateral-movement indicators.

Scenario professionale

Una credenziale valida sembra usata in modo anomalo ma senza alert critici: avviare una caccia mirata. 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: Hunt finding rate, account anomalies confermate, privileged misuse detected.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Fiducia eccessiva nell'EDR out-of-box, analisi isolata per host.

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 "Endpoint, identity e lateral movement hunting".

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**Cloud e SaaS hunting**

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

Executive briefing

Estendere il threat hunting a control plane, workload, IAM e applicazioni SaaS.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Costruire ipotesi specifiche per abuse di cloud roles, OAuth consent, data staging e admin changes.

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: Costruire ipotesi specifiche per abuse di cloud roles, OAuth consent, data staging e admin changes.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Cloud hunt playbook, IAM anomaly queries, SaaS admin-event review.

Scenario professionale

Un attacker usa un'applicazione OAuth legittima per persistere: definire la caccia. 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: Hunts cloud completati, anomalie IAM confermate, nuove detection create.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Focus solo su endpoint, cloud logs ignorati, SaaS fuori perimetro analitico.

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 "Cloud e SaaS hunting".

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**Reporting tecnico e trasformazione in detection**

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

Executive briefing

Trasformare i risultati di hunting in decisioni, detection e miglioramento del controllo.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Documentare conclusioni, confidenza, limiti, azioni e priorità di follow-up.

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: Documentare conclusioni, confidenza, limiti, azioni e priorità di follow-up.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Hunt report, detection backlog, corrective actions, residual-risk note.

Scenario professionale

Un hunt individua lacune ma nessuno le traduce in azioni: chiudere il ciclo. 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: Detection derivate da hunt, lead time di implementazione, improvement closure rate.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Report narrativi senza action item, scarsa riusabilità dei risultati.

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 tecnico e trasformazione in detection".

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**Programma continuo, skill e governance**

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

Executive briefing

Portare il threat hunting da iniziativa sporadica a programma continuo con skill e regole.

Competenze specialistiche attese

Il modulo è progettato per operatori che devono trasformare il tema in design, configurazioni, procedure e decisioni tecniche difendibili. Focus: Pianificare capacità, training, cadenza, backlog e integrazione con SOC/IR.

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: Pianificare capacità, training, cadenza, backlog e integrazione con SOC/IR.

Configurazioni, prove ed evidenze

L'adozione matura richiede evidenze tecniche, operative e decisionali. Evidenze chiave: Program roadmap, role matrix, quarterly plan, governance review.

Scenario professionale

L'organizzazione vuole "fare hunting" ma non alloca tempo e responsabilità: costruire 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: Ore dedicate, output riusabili, top hypotheses coverage, maturity progression.

Errori da evitare

I programmi specialistici falliscono spesso per superficialità tecnica o per governance debole. Evitare: Hunting relegato al tempo libero, nessuna governance, obiettivi mobili.

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 "Programma continuo, skill e governance".

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: THREAT-HUNTING
- 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.