



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

Threat Hunting & Detection Engineering Specialist

Course + certificate

On request

VAT excluded

Course code

THREAT-HUNTING

Minimum duration

424 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Specialist pathway for professionals who want to conduct structured threat hunting, hypothesis-driven detection engineering and analysis of indicators, behaviours and anomalies.

This extended technical dossier describes the pathway as published in CIWZ Academy on the issue date. It consolidates purpose, references, learning architecture, module contents, assessment system, passing criteria and certificate conditions. It does not replace the official texts of the standards, laws, guidelines or schemes referenced.

2. Normative, regulatory and technical references

MITRE ATT&CK; Pyramid of Pain; YARA; Sigma; hunting tradecraft best practices

References are used as the learning and assessment framework within the limits of published content and available sources. For professional application, the official and current versions of the referenced documents always prevail.

3. Learning architecture and assessment system

- 8 structured learning modules
- minimum tracked time: 424 min
- intermediate-check bank: 256 questions
- active final-exam bank: 240 questions
- final exam: 30 questions selected from the bank
- passing threshold: 75%
- Access to the pathway through the personal Academy profile or a corporate assignment.
- Sequential study of the modules, with server-side recording of progress and required minimum time.
- Intermediate checks linked to modules to verify understanding, application capability and quality of reasoning.

- Final exam unlock only after the pathway requirements have been completed.
- Protected final exam assembled by the platform through selection from the active course question bank.
- Recording of the result and, where applicable, the option to request the final certificate.

4. Official catalogue technical information

Course technical sheet

Specialist CIWZ Academy pathway with original content, server-tracked lessons, 8 modules, randomized intermediate checks, protected final assessment and a scenario-based question bank. Indicative average market benchmark: EUR 1,950 (typical range EUR 1,290 – EUR 2,790). Free access; any fee applies only to certificate issuance after passing.

5. Detailed course syllabus

The following syllabus is derived from the active modules published on the platform. Each module shows its minimum study time and the size of its available intermediate-check bank.

01 Threat-hunting mindset and hypothesis definition

Minimum time: 53 min | Intermediate questions: 32

02 Data preparation, pivots and enrichment

Minimum time: 53 min | Intermediate questions: 32

03 Behaviour analytics and ATT&CK-based hunting

Minimum time: 53 min | Intermediate questions: 32

04 YARA, Sigma and detection content

Minimum time: 53 min | Intermediate questions: 32

05 Endpoint, identity and lateral-movement hunting

Minimum time: 53 min | Intermediate questions: 32

06 Cloud and SaaS hunting

Minimum time: 53 min | Intermediate questions: 32

07 Technical reporting and conversion into detections

Minimum time: 53 min | Intermediate questions: 32

08 Continuous program, skills and governance

Minimum time: 53 min | Intermediate questions: 32

6. Developed module-by-module contents

The following pages analytically describe the content actually associated with each platform module. The structure is designed so that learners, companies, HR, Quality, HSE or CISO functions can understand precisely what is studied and assessed.

MODULE 01**Threat-hunting mindset and hypothesis definition**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Move from random hunting to hunting driven by hypotheses, data and risk priorities.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Generate hypotheses from threats, assets, exposure and reliable intelligence.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Generate hypotheses from threats, assets, exposure and reliable intelligence.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Hunting charters, priority matrices, hypothesis backlogs and target scope.

Professional scenario

The team “hunts” but without a clear purpose: introduce method and priorities. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Validated hypotheses, closed cycles, percentage of hunts linked to top risks.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Opportunistic hunting, vague objectives, non-reusable results.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme “Threat-hunting mindset and hypothesis definition”.

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 02**Data preparation, pivots and enrichment**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Prepare the right data to move quickly across endpoints, network, identity and cloud.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use pivots, timelines, enrichment and repeatable query patterns.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use pivots, timelines, enrichment and repeatable query patterns.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Data dictionaries, pivot playbooks, query libraries and entity mappings.

Professional scenario

A potential attack chain requires data from disconnected sources: build the links. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Average time to a meaningful pivot and coverage of useful data sources.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Misaligned data, inconsistent timestamps, unnormalized entities.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Data preparation, pivots and enrichment".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 03**Behaviour analytics and ATT&CK-based hunting**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Hunt for hostile behaviour rather than single IOCs, linking it to tactics and techniques.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply ATT&CK-based queries, behaviour chains and baseline deviations.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Apply ATT&CK-based queries, behaviour chains and baseline deviations.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: ATT&CK coverage maps, hunt queries, behaviour libraries and baseline evidence.

Professional scenario

Historical IOCs produce no results but risk remains high: move to behaviour hunting. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Coverage of top techniques, hit ratio, hunts converted into detections.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: IOC-only mindset, hunting disconnected from threat scenarios.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Behaviour analytics and ATT&CK-based hunting".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 04**YARA, Sigma and detection content**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Develop reusable content for memory, files, logs and behaviour.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Create and maintain YARA/Sigma rules aligned with hunts and detection pipelines.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Create and maintain YARA/Sigma rules aligned with hunts and detection pipelines.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Rule repositories, version history, validation notes and false-positive analysis.

Professional scenario

A rule is useful in the lab but impractical in production: make it sustainable. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Rule precision, deployment success, hunt-to-detection ratio.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Unversioned content, missing tuning, unvalidated rules.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "YARA, Sigma and detection content".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 05**Endpoint, identity and lateral-movement hunting**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Recognize endpoint-compromise patterns and lateral movement across identities and systems.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use process trees, auth events, privilege changes, admin tools and session trails.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use process trees, auth events, privilege changes, admin tools and session trails.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Process evidence, auth pivots, account-behaviour analysis and lateral-movement indicators.

Professional scenario

A valid credential appears to be used anomalously but without critical alerts: start a targeted hunt. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Hunt-finding rate, confirmed account anomalies, detected privileged misuse.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Overreliance on out-of-box EDR, analysis isolated per host.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Endpoint, identity and lateral-movement hunting".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 06**Cloud and SaaS hunting**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Extend threat hunting to control plane, workloads, IAM and SaaS applications.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Build hypotheses specific to cloud-role abuse, OAuth consent, data staging and admin changes.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Build hypotheses specific to cloud-role abuse, OAuth consent, data staging and admin changes.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Cloud hunting playbooks, IAM anomaly queries and SaaS admin-event reviews.

Professional scenario

An attacker uses a legitimate OAuth application for persistence: define the hunt. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Completed cloud hunts, confirmed IAM anomalies, new detections created.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Endpoint-only focus, cloud logs ignored, SaaS outside the analytic perimeter.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Cloud and SaaS hunting".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 07**Technical reporting and conversion into detections**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Turn hunting results into decisions, detections and control improvement.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Document conclusions, confidence, limitations, actions and follow-up priorities.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Document conclusions, confidence, limitations, actions and follow-up priorities.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Hunt reports, detection backlog, corrective actions and residual-risk notes.

Professional scenario

A hunt identifies gaps but nobody converts them into action: close the loop. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Detections derived from hunts, implementation lead time, improvement-closure rate.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Narrative reports without action items, poor reusability of outcomes.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Technical reporting and conversion into detections".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 08**Continuous program, skills and governance**

- Minimum required time: 53 min
- Available intermediate-check bank: 32 questions

Executive briefing

Move threat hunting from sporadic initiative to continuous program with skills and governance.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Plan capability, training, cadence, backlog and integration with SOC/IR.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Plan capability, training, cadence, backlog and integration with SOC/IR.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Program roadmaps, role matrices, quarterly plans and governance reviews.

Professional scenario

The organization wants to “do hunting” but allocates neither time nor responsibility: build the model. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Dedicated hours, reusable outputs, top-hypothesis coverage, maturity progression.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Hunting relegated to spare time, no governance, moving targets.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme “Continuous program, skills and governance”.

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

7. Assessment system, final exam and passing criteria

- Intermediate checks are linked to individual modules and provide progressive learning control before access to the final assessment.
- The final assessment consists of 30 questions selected from the active course bank. The platform applies an anti-repetition logic for new attempts when the bank size allows it.
- Final question-bank size detected at generation time: 240 active questions.
- Published passing threshold for the course: 75%.
- Questions are intended to assess not only recall but also interpretation, application, evidence selection, scenario assessment and quality of decision-making, depending on the subject matter.

8. Tracking, learning continuity and session integrity

- Path status, completed modules and recorded time are managed server-side when the course uses the Academy learning mode.
- The platform allows the pathway to resume from the recorded point and retains the results of required checks.
- Assessment sessions may be subject to the integrity and proctoring controls enabled by the platform and described in the applicable usage rules.
- Technical and integrity events support assessment and do not replace professional judgement where human review is required.

9. Certificate, use and limitations

The CIWZ certificate, where provided by the pathway and requested after passing, records the result achieved in the stated CIWZ pathway or assessment. It does not automatically replace personnel certification, professional registration, statutory licence, legal qualification or credentials issued by third-party bodies where such requirements are imposed by the applicable scheme.

10. Commercial and tax conditions

- Course + certificate: On request VAT excluded.
- UAE VAT is applied to UAE customers according to billing data and the applicable tax rules.
- Any specific commercial terms, agreements or corporate orders override the public price only when formally accepted by Certificato IWZ FZCO.

11. Dossier document control

- Document automatically generated by CIWZ Academy from the course data published at the time of the request.

- Course code: THREAT-HUNTING
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.