



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

SOC Engineering, SIEM & Detection Specialist

Course + certificate

On request

VAT excluded

Course code

SOC-DETECTION-ENG

Minimum duration

456 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Technical pathway to design use cases, data sources, correlation rules, telemetry pipelines and operational SOC models that truly work.

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; detection engineering best practices; Sigma; OpenTelemetry; SOC operating-model guidance

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: 456 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 2,090 (typical range EUR 1,390 – EUR 2,890). 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 SOC mission and operating model

Minimum time: 57 min | Intermediate questions: 32

02 Telemetry architecture and data onboarding

Minimum time: 57 min | Intermediate questions: 32

03 Use-case design and detection-as-code

Minimum time: 57 min | Intermediate questions: 32

04 Correlation, enrichment and prioritization

Minimum time: 57 min | Intermediate questions: 32

05 Detection validation, purple teaming and coverage review

Minimum time: 57 min | Intermediate questions: 32

06 Triage, investigation and case management

Minimum time: 57 min | Intermediate questions: 32

07 SOAR, automation and operational-risk control

Minimum time: 57 min | Intermediate questions: 32

08 Reporting, continuous improvement and SOC economics

Minimum time: 57 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**SOC mission and operating model**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Define the SOC's role and boundaries with IT, incident response, threat intelligence and vulnerability management.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Establish service models, tiering, ownership and KPIs oriented toward effective detection.

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: Establish service models, tiering, ownership and KPIs oriented toward effective detection.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Operating model, escalation matrix, KPI/SLA and use-case governance.

Professional scenario

The SOC receives every alert without business prioritization: reset 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: Relevant alerts handled on time, high-severity backlog, triage quality.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: SOC without clear mandate, fragmented ownership, volume-only KPIs.

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 "SOC mission and operating model".

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**Telemetry architecture and data onboarding**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Build a reliable data architecture to collect, normalize and enrich security telemetry.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Select priority data sources, parsers, common schemas, enrichments and data-quality checks.

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: Select priority data sources, parsers, common schemas, enrichments and data-quality checks.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Data-source inventory, parser mapping, field completeness and onboarding checklists.

Professional scenario

Logs exist but cannot be queried coherently: fix the data pipeline. 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 critical sources, event loss, completeness of key fields.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Onboarding without prioritization, inconsistent fields, uncontrolled ingestion cost.

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 "Telemetry architecture and data onboarding".

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

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Translate threats, abuse and real cases into maintainable detection rules.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use ATT&CK, Sigma, hypothesis-driven design and versioned detections.

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 ATT&CK, Sigma, hypothesis-driven design and versioned detections.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Detection catalog, rule logic, ATT&CK mapping, version history and tuning notes.

Professional scenario

A useful rule produces too much noise: optimize without losing coverage. 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: Detection precision, false-positive rate, ATT&CK coverage of top risks.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Duplicate rules, chaotic naming, detections not versioned.

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

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**Correlation, enrichment and prioritization**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Increase SIEM value by correlating events, identities, assets, context and intelligence.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define scoring, suppression and enrichment using CMDB/EDR/IAM and business criticality.

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: Define scoring, suppression and enrichment using CMDB/EDR/IAM and business criticality.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Enrichment maps, scoring matrices, suppression logic and context dictionaries.

Professional scenario

Analysts see technical alerts but do not know which assets are critical: close the gap. 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: Alerts with business context, correct escalations, reduced noise rate.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Random correlations, unvalidated threat intelligence, priority drift.

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 "Correlation, enrichment and prioritization".

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

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Verify that detections actually work through controlled testing and periodic reviews.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use ATT&CK emulation, purple teaming, validation datasets and post-incident reviews.

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 ATT&CK emulation, purple teaming, validation datasets and post-incident reviews.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Test plans, validation results, simulation logs and detection-gap registers.

Professional scenario

A detection has existed for months but nobody has verified it fires: introduce assurance. 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: Percentage of validated detections, closed gaps, coverage per top scenario.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Untested rules, assumed coverage, improvement only reactive.

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 "Detection validation, purple teaming and coverage review".

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**Triage, investigation and case management**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Standardize triage, analysis pivots, handoffs and evidence collection across SOC tiers.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define runbooks, severity models, hypothesis discipline and decision logging.

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: Define runbooks, severity models, hypothesis discipline and decision logging.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Runbooks, case templates, evidence checklists and investigation notes.

Professional scenario

Two analysts handle the same alert in opposite ways: normalize the process. 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: MTTA, percentage of cases with complete evidence, ticket reopens.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Weak case management, poor notes, analyst-dependent severity.

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 "Triage, investigation and case management".

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**SOAR, automation and operational-risk control**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Automate where useful without increasing the risk of incorrect actions.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply human-in-the-loop, safe actions, rollback and automation-effectiveness metrics.

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 human-in-the-loop, safe actions, rollback and automation-effectiveness metrics.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: SOAR playbooks, approval flows, execution logs and rollback evidence.

Professional scenario

A playbook automatically disables critical accounts and causes operational harm: correct the design. 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: Successful automated runs, rollback rate, triage-time reduction.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Blind automation, ownerless playbooks, no testing or rollback.

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 "SOAR, automation and operational-risk control".

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**Reporting, continuous improvement and SOC economics**

- Minimum required time: 57 min
- Available intermediate-check bank: 32 questions

Executive briefing

Demonstrate SOC value through readable reporting and measurable improvement.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Balance coverage, timing, quality, cost and residual risk through management dashboards.

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: Balance coverage, timing, quality, cost and residual risk through management dashboards.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Executive dashboards, cost models, improvement roadmaps and governance minutes.

Professional scenario

The board sees only ticket counts and cannot understand SOC effectiveness: rebuild reporting. 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: MTTD/MTTR, top detection gaps, cost per use case, coverage trend.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Overly technical reporting, no prioritization, costs not linked to 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 "Reporting, continuous improvement and SOC economics".

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: SOC-DETECTION-ENG
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.