ACRAIS Research & Assessment Design

Cause-to-Symptom Security Verification

Evidence-led cybersecurity exercises connecting attack causes to observable logs, alerts, network activity, endpoint behaviour and system changes before conclusions are reached.

Verification chain

Security cause → resulting event → observable symptoms → supporting evidence → alternative explanation → conclusion → response action.

Evidence learners must correlate

Evidence area	Examples
Logs and identity	Authentication, application and cloud records
Alerts and endpoints	Detection signals, processes and device behaviour
Network activity	Connections, DNS and traffic changes
System changes	Accounts, privileges, tasks and configurations

Where this fits in ACRAIS

Verified intelligence informs governed scenarios. Learners practise correlation, complete practical assessments, pass automated integrity gates and enter human review where required. Only defensible results should progress into credentials and the Skills Passport.

Assessment direction

The design evaluates reasoning rather than recognition alone. Explicit causal-reasoning exercises and scoring should be introduced in controlled phases, with evidence quality, alternative explanations and response actions included in assessment criteria.

Implementation principle

Preserve the existing ACRAIS assessment and integrity architecture. Add cause-to-symptom scenarios as governed content and measure performance before broader rollout.