Operation Glass Harbor

Operation Glass Harbor is a fictional defensive lab with 12 stages. It puts different evidence types on one incident timeline.

WHERE IS DATA PROCESSED?
Runs on your device

GOAL

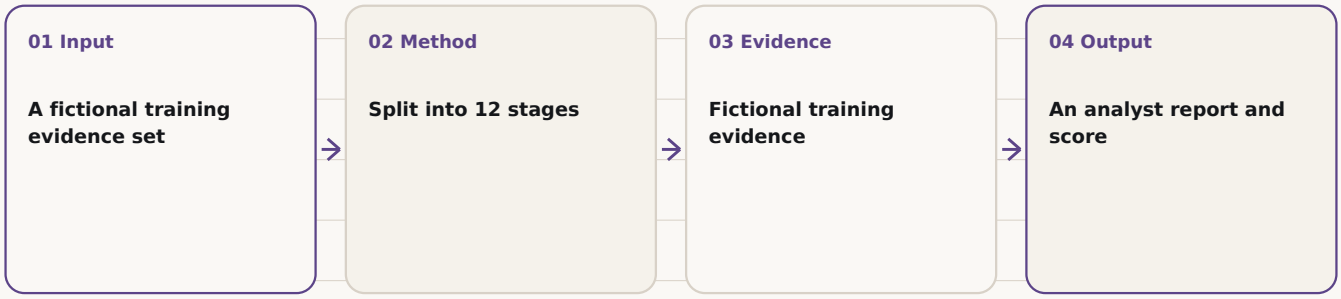
Gives step-by-step analyst practice on a fictional evidence set.

WHO IS IT FOR?

For people who want to practise joining different evidence types step by step in a safe, fully fictional incident.

TECHNICAL FLOW

Input, method, evidence, and output



Operation Glass Harbor

HOW DOES IT WORK?

Step 1

Build a fictional evidence set

The repository holds email, Git, TLS, DNS, visual, HUMINT, telemetry, and supply-chain files. Their source paths stay visible.

Step 2

Split into 12 stages

Each stage links one question, evidence group, expected method, and controlled flag value.

Step 3

Keep progress local

Stage status and analyst notes stay on this device, so the user can continue later.

Step 4

Score the evidence record

The system checks sources, method, and the minimum evidence record, not only the final answer.

Step 5

Validate the flag on the server

The submitted flag is checked with server-side HMAC validation, not a plain answer list in the browser.

Step 6

Build the analyst report

The report joins the completed stages. It includes a timeline and hypotheses. It also includes evidence strength, gaps, and defensive recommendations.

LIMITS

All people, organizations, and events are fictional. The lab is for defensive training and contains no real targets or credentials.