CSINT Incident Lab

The Incident Lab provides source validation, timeline, and reporting practice with fictionalized and sanitized incident files.

WHERE IS DATA PROCESSED?
Runs on your device

GOAL

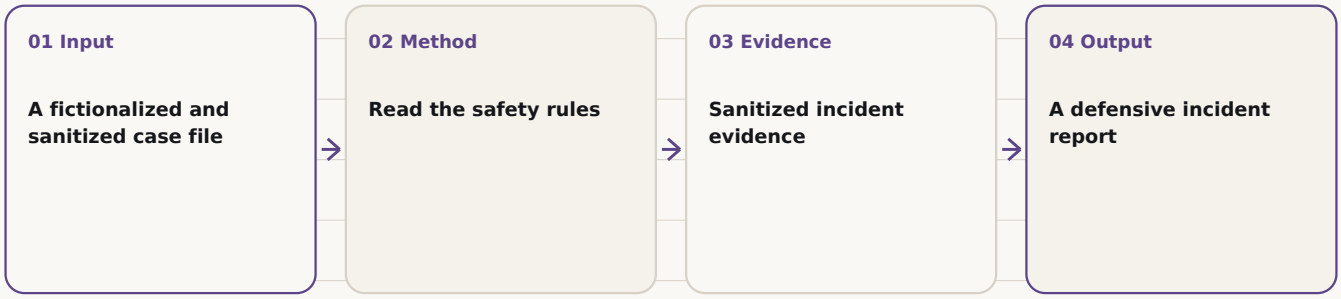
Provides incident-analysis and defensive-reporting practice with fictionalized and sanitized evidence.

WHO IS IT FOR?

For people who want to practise source validation and incident analysis with fictionalized and sanitized evidence.

TECHNICAL FLOW

Input, method, evidence, and output



CSINT Incident Lab

HOW DOES IT WORK?

Step 1

Choose a case

Choose a fictional case that matches your level and the method you want to practise.

Step 2

Read the safety rules

Check the training boundary, sanitized material, and prohibited actions before working the case.

Step 3

Review the evidence

Read items such as email, timestamps, network records, or incident notes together with their sources.

Step 4

Build a timeline

Order confirmed events and keep assumptions and gaps separate.

Step 5

Assess evidence strength

State which record supports each conclusion and which check is still missing.

Step 6

Write a defensive report

Combine findings, uncertainty, and a safe defensive recommendation in a short report.

LIMITS

The lab contains no real people, victims, live targets, or leaked data. It is not for unauthorized access, people tracking, or live-system testing.