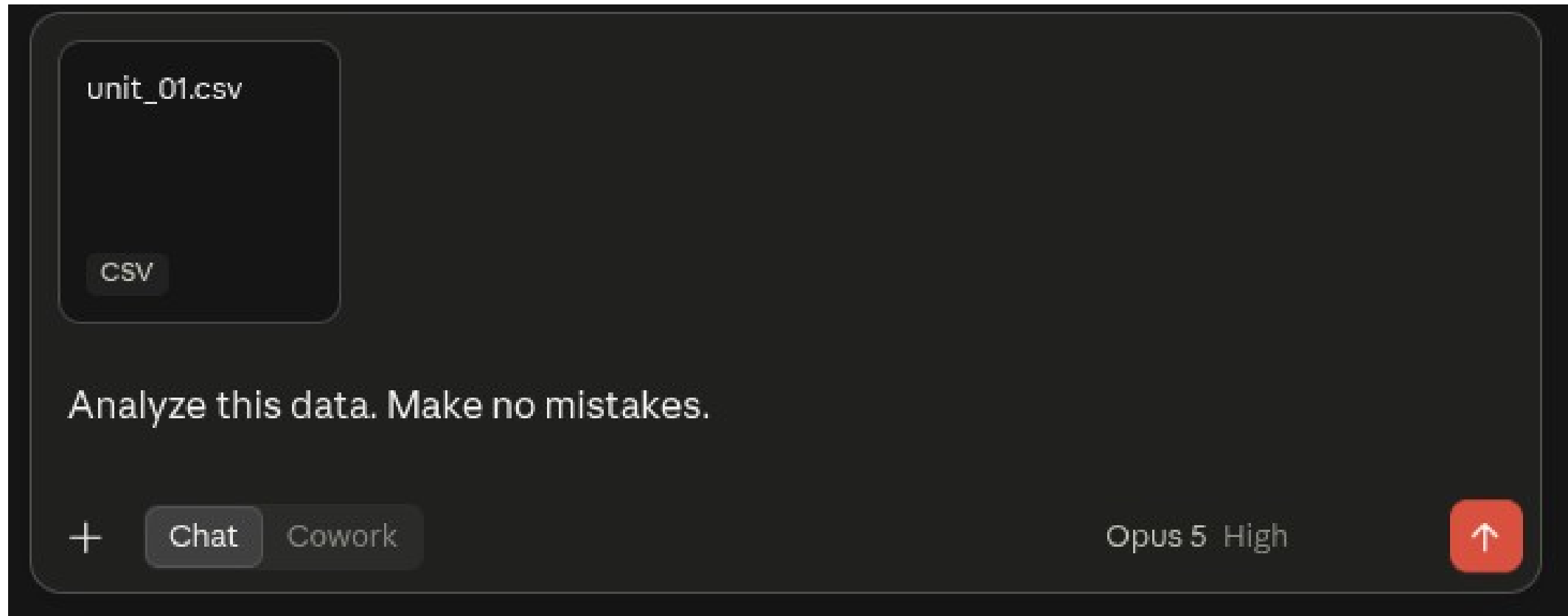


What could go wrong?



Introducing:

Confidentiality Broker

Problem

The data goes wherever the model is

OPERATOR'S ENVIRONMENT

EU

OUTSIDE THE EU

> what is wrong with unit_06?

sensordata/unit_06.csv

810 samples x 52 tags, raw

316 KB

google [public]

No record of what left, to which model, or why.

Nothing on this path asked whether it should happen, and nothing wrote down that it did.

Solution

The label decides how far anything goes

OPERATOR'S ENVIRONMENT	EU	OUTSIDE THE EU
> what is wrong with unit_06?  restricted-plant/ restricted lemonade, ollama the raw rows stay here  confidential-plant/reports/ confidential 8.6 KB of statistics, no rows	verda [confidential] ✓	google [public] ✗ no access Not the rows, not the statistics, not a file listing.

Raw rows never leave the machine. Derived statistics stop in the EU. The question still gets answered.

THE RULE

The folder decides which model sees it

The broker compares the folder's label with the provider's clearance, on every tool call.

demo/restricted-plant/ **restricted**

the raw rows: 18 recordings, 52 tags

lemonade, ollama

no cloud model, not even the EU one

demo/confidential-plant/ **confidential**

the derived fingerprints the audit produced

mistral, verda, lemonade, ollama

the Finnish endpoint may, Google may not

Raw rows never leave this machine. Data minimization is two labels on two folders, not a sentence in a prompt.

Demo