Detection pack

Prepares detection content from current threat records.

PROCESSING BOUNDARY
Reads public open-source feeds

PURPOSE OF THE SITE

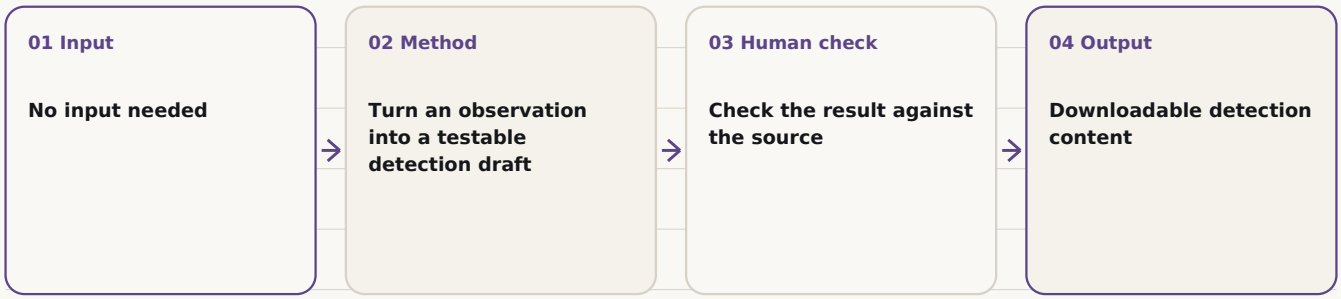
This site exists to turn one question into a safe, repeatable research process. A tool result is not a verdict; the source and the human check stay visible.

WHY DID I BUILD IT?

I built this to keep the observation, logic, data requirement, and test note together instead of copying a CTI record straight into a rule.

SMALL ARCHITECTURE

Four parts from input to a record you can keep



Detection pack

USE IT STEP BY STEP

Step 1

Prepare the material

Start with: No input needed

Step 2

Turn an observation into a testable detection draft

Prepares detection content from current threat records.

Step 3

Check the result against the source

Map fields to your own log schema and test the rule with synthetic or approved historical data. Do not ship an untested draft.

Step 4

Download and keep the record

Keep this at the end: Downloadable detection content

HONEST BOUNDARY

The output is a detection draft. It is not ready for every SIEM, does not know its false-positive rate, and does not make blocking decisions.