IOC lookup

Checks an indicator against open-source records.

PROCESSING BOUNDARY
The query goes through a server proxy

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 compare public records for an IP, domain, URL, or hash without losing the source and date context.

SMALL ARCHITECTURE

Four parts from input to a record you can keep

01 Input
An IP, domain, or hash

→

02 Method
Classify the observable and query the right source

→

03 Human check
Check the result against the source

→

04 Output
A source-by-source reputation summary

IOC lookup

USE IT STEP BY STEP

Step 1

Prepare the material

Start with: An IP, domain, or hash

Step 2

Classify the observable and query the right source

Checks an indicator against open-source records.

Step 3

Check the result against the source

Check the match date, observable type, and source description. Do not read an old or shared IP record as current attacker identity.

Step 4

Download and keep the record

Keep this at the end: A source-by-source reputation summary

HONEST BOUNDARY

No public match does not prove an observable is clean. A match alone also does not explain the incident context.