

[Research files](#)[Work](#)[E-library](#)[About](#)[TR](#)[EN](#)

IOC Lookup

IOC Lookup

Paste an IP, domain, hash, or URL. See what open sources say, what is still unknown, and what you can put in a note.

Live open sources only. The query goes through a CSINT server.

01 Paste

02 Check

03 Read

04 Copy

Indicator to check

IOC: IP, domain, file hash, or web address.

How the threat intelligence pipeline is built

The threat intelligence pipeline is a background service that collects public security records at regular intervals, removes duplicates and brings important changes forward. It has no page of its own. This handbook explains how the pipeline works and where its output appears on the site.

1 A pipeline, not a page

You cannot follow every new vulnerability, every vendor advisory and every new indicator list by hand. The same event can also appear under different names in several sources. I built this pipeline for that. It reads the sources, turns them into one format, merges duplicates and records what has really changed.

The pipeline is a Worker running on Cloudflare. Visitors do not trigger anything. The Worker runs on a timer by itself and writes the result to a database. Pages on the site read that result.

The pipeline has no page of its own. Its output appears in the live feed section of the Threat actors page, on the Android threats page and on the source changes page. That is why the screenshots in this handbook come from those pages and from the IOC desk.

A few words

CVE	The standard number given to a disclosed security flaw.
KEV	CISA's list of flaws known to be exploited in the real world.
EPSS	FIRST's published estimate of how likely a flaw is to be exploited soon.
CVSS	A score from 0 to 10 for the technical weight of a flaw.
IOC	A trace that points to an attack. It can be an IP address, domain, file hash or web address.

2 Sources and schedule

CISA KEV	Flaws known to be exploited. If the main address does not open, CISA's GitHub copy is read.
NVD	The US national vulnerability database. At most 50 records per run.
FIRST EPSS	Estimates of how likely flaws are to be exploited. Read not as separate records but as extra data on CVE records.
CISA CSAF	CISA's machine-readable security advisories, taken from changes in its GitHub repository.
Microsoft Security	The RSS feed of the Microsoft security blog. Indicators are extracted only from this and the next source.
Google and Mandiant	The RSS feed of the Google and Mandiant threat intelligence blog.

Every 5 minutes	Daily 05:00 UTC	When a page opens
Sources are read, records are cleaned up and written to the database.	Priorities are worked out again and the daily briefing is produced.	The browser only reads the finished result. No request goes to the sources on the visitor's behalf.

For each source the Worker waits at most 20 seconds and reads at most 2.5 MB. For NVD the limit is 4 MB. If one source does not answer, the others keep going.

3 Cleaning, duplicates and change

- 1

One format
Every source is turned from its own format into a common record. The title is capped at 320 characters, the summary at 1400. Dates are put into one format.
- 2

Stable ID
A record's ID is made with SHA-256 from the source name and the source's own number. When the same record comes again, no new record is opened.
- 3

Update only on change
A separate digest is taken of the record's content. If it has not changed, nothing is written. If it has, the record is updated and each version is kept in a separate table.
- 4

Merging indicators
If the same IP, domain or file hash appears in different sources, it is kept as one indicator. First and last seen dates, sources and related CVEs are merged.
- 5

Material change
An indicator being added or removed, a flaw entering KEV, EPSS rising, a change in affected products, remediation advice or CVSS, and an advisory being withdrawn are recorded separately. These records are kept for 180 days.

4 Priority score

Every CVE gets a score from 0 to 100. The formula is written openly in the code. There is no hidden model or AI decision.

In KEV or actively exploited	+55
Known to be used by ransomware	+20
EPSS 0.5 or more, 0.1 or more, 0.01 or more	+20, +12, +5
CVSS 9 or more, 7 or more, 4 or more	+15, +10, +5
Published in the last 7 days	+5
Level	70 and above urgent, 50 and above today, 10 and above watch, below that low.

The score is a ranking aid. It does not know whether the flaw exists in your systems. It is not a final risk decision, an attribution or an automatic response decision.

5 Where it shows on the site

The screenshot shows a web interface for a live threat feed. At the top, there is a toggle switch labeled 'Show new incidents and advisories'. Below this, a section titled 'Live threat feed' contains a sub-header 'New incidents and advisories' and a note: 'CISA, NVD, FIRST, Microsoft, and Google/Mandiant sources are checked every five minutes.' To the right of this section, a status indicator says 'Live, Updated now'. Below the note, there are four filter dropdown menus: 'All events', 'All sources', 'All levels', and 'All actors'. At the bottom, a list of incidents is displayed, each with a CVE ID, a brief description, a severity level (Medium or High), and a timestamp (NVD, 30 Sept 2026, 14:16). The incidents are: CVE-2026-96342 (Missing Authorization vulnerability in Amauri.IO WPMobile.App wpappninja al...), CVE-2026-76992 (The CODESYS Gateway Client allocates memory based on a size field in a gate...), and CVE-2026-13720 (An Editor can set file-provisioning metadata (the grafana.app/managedBy, gr...)).

The threat feed on the live site. Real events from the sources are listed below the filters. Titles remain in the source's own language.

1 Where the feed comes from

The section says which sources are checked and how often.

2 Filters

Filter by event type, source, severity, actor and sector. Filtering goes to the Worker as a query.

3 Status

When the feed cannot be reached, it says so plainly and does not show an old list as if it were new. The browser refreshes the list once a minute.

The Worker offers read endpoints for the feed, a dashboard summary, changes, a single event and the daily briefing. The briefing is produced and stored once a day by Istanbul date. It holds the counts for the last 24 hours, the top 5 events, 5 CVEs, 10 indicators, 6 sectors and up to 5 remediation steps. Today no page on the site shows the briefing directly.

6 The next step, the IOC desk

The pipeline gives the overall picture. When you want to ask about a single indicator, you move to the IOC desk. The desk uses a separate Worker and runs only when you ask.

Indicator to check
IOC: IP, domain, file hash, or web address.

1

2 Type: Leave on auto if you are unsure. ▼

3 **No query yet**
Paste one IP, domain, hash, or URL above. The result is built only from sources retrieved right now.

The IOC desk, before a query.

1 Indicator

An IP, domain, file hash, web address or CVE. Private network addresses are refused. If you give a web address, only the domain is resolved and the page is not opened.

2 Type

Leave it on auto if you are unsure. The type decides which public sources are asked.

3 Result

Built only from sources fetched at that moment. A source whose key is not set up is not queried, and that is stated plainly.

The desk does not write results to a database. To avoid asking the same question again, a result is kept briefly in the Cloudflare cache. That time is 6 hours for file hashes and CVEs and 15 minutes for the rest. The cache key is built from the SHA-256 digest of the indicator and does not contain the indicator itself. There is a limit of 20 queries a minute per IP.

7 What it does not do

- ✗ It reads only published sources and explicitly written indicators. It does not look at closed forums or leaked data.
- ✗ The priority score does not know your environment. It does not say whether a flaw exists on your side.
- ✗ It does not tie an indicator to a group or a country. Attribution is an analyst's decision.
- ✗ If a source is wrong, the record is wrong too. Every record carries its source address, so go back to the source before important decisions.