CTI / FORECAST

FOR TECHNICAL TEAMS

Technical datasheet and integration guide

Data, API, TAXII 2.1, STIX 2.1, integrations, security and operations: the reference for technical teams.

SHAREABLE

Audience
CISOs, SOC teams, administrators, integrators

Version
1.0 · 7 November 2026

Support
contact@ctiforecast.com

Contents

01 Service overview
02 Data collection and processing
03 Data model
04 Confidence and decay
05 API access
06 Endpoint reference
07 TAXII 2.1 and STIX 2.1
08 Integration guides
09 Security and privacy
10 Availability and support
11 Frequently asked questions

01 Service overview

CTI Forecast provides a feed of indicators of compromise (IOCs) and vulnerability exploitation forecasts, available through a REST API, a TAXII 2.1 server, STIX 2.1 bundles and plain-text blocklists. This document describes the data, the interfaces, common integrations, security and operations, for the teams who deploy the service.

FEATURE	VALUE
Indicator types	`ip` (IPv4/IPv6), `domain`, `url`, `sha256`, `sha1`, `md5`, `cve`
Sources	339 research sources (vendors, CERTs, labs) and curated feeds (ESET malware-ioc, abuse.ch Feodo Tracker and SSL Blacklist)
Volume	Over 257,000 published indicators (November 2026)
Freshness	Synchronised every 5 minutes (Pro and Business plans)
Enrichment	Confidence 0-100, source and articles, ASN, operator and country for IPs, malware family when known
Interfaces	JSON REST API (OpenAPI 3.1), TAXII 2.1, STIX 2.1, plain text, CSV
Data hosting	France; delivered through Cloudflare
Specification	`https://ctiforecast.com/openapi.json`

02 Data collection and processing

1. **Collection**: continuous reading of security research publications; extraction of candidates (IPs, domains, URLs, hashes, CVEs), including defanged forms (`hxxp` , `[.]`).
2. **Filtering**: removal of known false positives:
   - legitimate domains: major services, email providers, and the 10,000 most visited websites (Tranco list, refreshed weekly);
   - CDN and major-service IPs; non-routable ranges; public resolvers; version numbers mistaken for IPs;
   - file extensions mistaken for domains (`config.json`); the domains of the source websites themselves.
3. **Scoring**: confidence score based on source type, corroboration, repetition and network type (section 4).
4. **Cross-checking** with curated feeds and, for CVEs, with EPSS (FIRST) and the CISA KEV catalog.
5. **Publication**: only indicators above the thresholds are served; their confidence decays over time.

The collector only reads publications: it never interacts with attacker infrastructure. Fewer than one candidate in five passes the filters.

03 Data model

Indicator (`/v1/iocs` , `/v1/lookup` , `/v1/export`)

FIELD	TYPE	DESCRIPTION
`value`	string	Value, not defanged in the API
`type`	string	`ip` , `domain` , `url` , `sha256` , `sha1` , `md5` , `cve`
`confidence`	integer 0-100	Current confidence, after decay
`confidence_base`	integer 0-100	Original confidence, before decay
`severity`	integer or null	Severity estimated by the collector
`first_seen` , `last_seen`	ISO 8601 (UTC)	First and last sighting
`mentions`	integer	Number of sightings
`source`	string	Main source
`category` , `malware_family`	string or null	Category and family, when known
`asn` , `as_name` , `country`	IP only	Autonomous system, operator, country (ISO 3166-1)
`references`	list	Up to 3 sources (5 for a lookup): `url` , `source` , `seen_at` , plus `context` and `curated: true` for curated feeds. Empty on Free

CVE forecast (`/v1/forecast` , `/v1/cve/{id}`)

FIELD	DESCRIPTION
`signal`	`exploitee` (already in KEV), `imminente` (likely soon), `a_surveiller` (watch), `faible` (low)
`signal_label`	Human-readable label, in the language of `Accept-Language`
`forecast_score`	Rank 0-100 among tracked CVEs
`kev_probability_30d`	Estimated probability of a KEV addition within 30 days
`epss` , `epss_percentile` , `epss_date`	EPSS data of the day
`in_kev` , `kev_date_added` , `kev_ransomware_use`	Status in the CISA catalog
`mentions_7d` , `mentions_previous_7d` , `active_days_7d`	Publication dynamics

`reasons`	Readable explanation of the score (currently in French)

04 Confidence and decay

The confidence score (0-100) summarises how reliable an indicator is. For IPs, it combines:

- the **source type**: curated feed published by the vendor (strong), research lab, specialised media, security advisory (weak);
- **corroboration** by several independent sources;
- **repeated sightings** and severity;
- the **network type** (ASN): VPS hosting (higher), public cloud (slightly lower); CDN and major-service IPs are never published.

Decay

Without a new sighting, confidence halves after **30 days** for IPs and URLs and after **90 days** for domains, following a 7-day grace period. File hashes and CVEs do not decay. The original value remains available in `confidence_base`.

Recommended thresholds

USE CASE	RECOMMENDED MIN_CONFIDENCE
Automatic blocking (firewall, DNS filtering)	≥ 70 (default for blocklists)
SIEM alerting	≥ 50
Enrichment, threat hunting	≥ 40 (minimum served for IPs)

> **Good practice**
> Start in alert mode (no blocking) for one to two weeks, review matches against your logs, then enable blocking. Keep a local exception list for your partners.

05 API access

General

ITEM	VALUE
Base URL	`https://ctiforecast.com`
Format	UTF-8 JSON; ISO 8601 dates in UTC
Authentication	`X-API-Key: <key>` header (recommended), `Authorization: Bearer <key>`, Basic (password = key, for TAXII), or `?key=` for tools that cannot send headers
Keys	Created under “My account”, shown only once, revocable; several keys allowed (one per tool)
Quotas	Free 100, Pro 10,000, Business 100,000 requests per day; reset at midnight UTC
Quota headers	`X-RateLimit-Limit`, `X-RateLimit-Remaining`
Message language	Based on `Accept-Language` (`en` or `fr`)

Response codes

CODE	MEANING
200	Success
400	Invalid parameter (message in `error`)
401	Missing, invalid or revoked key
403	Feature or type not included in your plan
429	Daily quota reached

Pagination and incremental collection

`/v1/iocs` returns indicators from newest to oldest. For the next page, pass the `next_until` value as the `until` parameter. For incremental collection, store the time of your last run and pass it as `since`.

```
curl -H "X-API-Key: $CTI_KEY" -H "Accept-Language: en" \
  "https://ctiforecast.com/v1/iocs?type=ip,domain&min_confidence=70&since=2026-11-06T00:00:00&limit=
1000"
```

06 Endpoint reference

ROUTE	PARAMETERS	RESPONSE	PLAN
`GET /v1/iocs`	type, since, until, min_confidence, limit (max 100 / 1,000 / 5,000)	`count`, `next_until`, `delayed_hours`, `data[]`	All
`GET /v1/lookup`	value (required)	`found`, `matches[]`	All
`GET /v1/stats`	—	Plan, volumes, today's quota	All
`GET /v1/blocklist.txt`	type (ip, domain, url, sha256, sha1, md5), days (1-365, 30), min_confidence (70)	Plain text, one value per line	Types in your plan
`GET /v1/trending`	type, status (nouveau, en_hausse, stable, en_baisse), min_confidence, limit	Accelerating indicators (7 days vs 7 days)	Free: top 10
`GET /v1/forecast`	signal, min_score, limit	CVEs ranked by probability	Free: top 10
`GET /v1/cve/{{id}}`	CVE identifier	Full record	All
`GET /v1/stix`	same as /v1/iocs	STIX 2.1 bundle	Pro, Business
`GET /v1/export`	same as /v1/iocs + format (csv, json)	Up to 500,000 rows	Business

Sample response (`/v1/lookup`)


```
{"value": "185.177.93.120", "found": true, "matches": [{
  "value": "185.177.93.120", "type": "ip", "confidence": 74, "confidence_base": 74, "severity": 70,
  "first_seen": "2026-10-28T09:12:40", "last_seen": "2026-11-06T21:20:11", "mentions": 10,
  "asn": 211138, "as_name": "…", "country": "NL",
  "references": [{"url": "https://www.bitdefender.com/…", "source": "www.bitdefender.com", "seen_a
t": "2026-11-06T21:20:11"}]}]}
```


Illustrative values. The full specification, with every schema, is available at `/openapi.json`.

07 TAXII 2.1 and STIX 2.1

TAXII server (read-only, Pro and Business)

ITEM	VALUE
Discovery	`https://ctiforecast.com/taxii2/`
API root	`https://ctiforecast.com/taxii2/api/`
Authentication	Basic: any username, password = API key
Filters	`added_after` , `match[type]` , `limit` ; pagination with `next`

COLLECTION	IDENTIFIER	CONTENT
Malicious IPs	`77653c02-ccd7-55e5-8db8-85d421cfba7c`	IPv4 / IPv6
Malicious domains and URLs	`6d85c187-7ce5-561a-9cb0-d820a89fd099`	domain, url
Malicious files	`60ef1a80-e85a-56e8-84b6-f6e51e8d3fb6`	sha256, sha1, md5
Vulnerabilities	`00ae1b11-d2b2-550f-91d2-39efc6c29dd7`	CVE

STIX 2.1 mapping

- Each IOC becomes an `indicator` object (`pattern_type: stix` , `indicator_types: malicious-activity`); CVEs become `vulnerability` objects.
- Patterns: `[ipv4-addr:value = '…']` , `[ipv6-addr:value = '…']` , `[domain-name:value = '…']` , `[url:value = '…']` , `[file:hashes.'SHA-256' = '…']` .
- `confidence` carries the score; `valid_until` follows the decay; **TLP:GREEN** marking; source articles as `external_references` .
- Stable identifiers: re-importing updates existing objects instead of creating duplicates.
- Compliance checked with the official OASIS libraries (`stix2` , `taxii2-client`).

08 Integration guides

In the examples, replace `YOUR_KEY` with a key dedicated to the tool. URLs containing the key give access to your account: do not publish them.

pfSense / OPNsense

Firewall → **Aliases** → **URLs** (OPNsense: **Firewall** → **Aliases**, URL Table type), name `CTI_FORECAST_IP`, daily refresh, URL:

```
https://ctiforecast.com/v1/blocklist.txt?type=ip&days=30&key=YOUR_KEY
```

Then create a **Block** rule on the WAN interface (inbound) and LAN (outbound) using this alias.

Wazuh (CDB list)

```
curl -fsS "https://ctiforecast.com/v1/blocklist.txt?type=ip&days=30&key=YOUR_KEY" \
  | grep -v '^#' | sed 's/$/:cti-forecast/' > /var/ossec/etc/lists/cti-forecast-ip.tmp \
  && mv /var/ossec/etc/lists/cti-forecast-ip.tmp /var/ossec/etc/lists/cti-forecast-ip \
  && systemctl restart wazuh-manager
```

Declare `<list>etc/lists/cti-forecast-ip</list>` in `ossec.conf` and add a rule with `<list field="srcip" lookup="address_match_key">`.

OpenCTI

TAXII2 connector: `TAXII2_DISCOVERY_URL=https://ctiforecast.com/taxii2/`, `TAXII2_USERNAME=client`, `TAXII2_PASSWORD=YOUR_KEY`, `TAXII2_V21=true`, `TAXII2_COLLECTIONS=*.*`.

Microsoft Sentinel

Content hub → *Threat Intelligence* solution → *Threat Intelligence - TAXII* connector: API root `https://ctiforecast.com/taxii2/api/`, collection ID (section 7), username `client`, password = key, hourly polling.

MISP

Sync Actions → Feeds → Add Feed, *Freetext Parsed Feed* format, one feed per type:

```
https://ctiforecast.com/v1/blocklist.txt?type=sha256&days=7&key=YOUR_KEY
```

Splunk

```
{ echo "ioc"; curl -fsS "https://ctiforecast.com/v1/blocklist.txt?type=ip&key=YOUR_KEY" | grep -v '^
#'; } \
  > $SPLUNK_HOME/etc/apps/search/lookups/cti_forecast_ip.csv
```

Then: `| lookup cti_forecast_ip.csv ioc AS src_ip OUTPUT ioc AS cti_match | where isnotnull(cti_match)`

Other tools

Elastic, QRadar, TheHive, Python scripts, n8n: any tool that can send an HTTP request can use the JSON API. Generate a client from `/openapi.json` with *openapi-generator*.

09 Security and privacy

AREA	MEASURE
Transport	HTTPS only, TLS 1.2 minimum, HSTS
API keys	Stored as irreversible hashes; shown only once; revocable at any time
Accounts	Hashed passwords; two-factor authentication (TOTP) available; login throttling
Looked-up values	**Never stored**: neither in the database nor in logs (logs do not record URL parameters)
Data kept	Account (email, company), number of requests per day, billing (Stripe)
Infrastructure	No inbound port exposed to the Internet; access through the Cloudflare network
Backups	Encrypted (AES-256) before upload, stored in France, immutable for 30 days
GDPR	DPA (Article 28) published: ctiforecast.com/en/dpa; signed copy on request
Responsible disclosure	security@ctiforecast.com; policy at ctiforecast.com/en/security; `/.well-known/security.txt`

Recommendations

- Use one key per tool, so you can revoke one without breaking the others.
- Prefer the `X-API-Key` header over the `?key=` parameter when the tool allows it.
- Enable two-factor authentication on the account that manages the keys.

10 Availability and support

ITEM	CURRENT COMMITMENT
Data freshness	Synchronised every 5 minutes; curated feeds every 6 hours; forecasts daily
Monitoring	Automatic checks every 5 minutes (synchronisation, collection, forecasts, backups, disk)
Public status page	stats.uptimerobot.com/J8ZkzyVqvK
Support	contact@ctiforecast.com, reply within one business day (French or English)
Contractual SLA	Not offered at this time; considered case by case for custom offers
Changes	Announced at ctiforecast.com/en/changelog, in advance when they affect the API

Robustness tips

- Poll blocklists at most hourly: they do not change faster than the synchronisation.
- On network errors or 5xx responses, keep the last valid list and retry later with an increasing delay.
- Watch `X-RateLimit-Remaining` to stay within your quota.

11 Frequently asked questions

QUESTION	ANSWER
Are values defanged?	Not in the API and lists (so your tools can use them). They are on the website (`example[.]com`).
Why did an IP disappear from the list?	Its confidence fell below the threshold through decay, or it was recognised as legitimate (CDN, major service).
Can I report a false positive?	Yes: contact@ctiforecast.com, with the value and the context. It is reviewed and may improve the filters for everyone.
What is the difference between Free and Pro?	Free: CVE and SHA-256 only, 24-hour delay, no sources. Pro: every type, real time, sources, TAXII and STIX.
Can I test without signing up?	Yes: CSV sample at ctiforecast.com/en/sample. The 14-day Pro trial requires no credit card.
Can the data be redistributed?	For use within your organisation. Any redistribution outside it (for example an MSSP serving its customers) requires written agreement, provided in custom offers. See the terms of sale.
What is the TLP marking?	STIX indicators are marked TLP:GREEN (may be shared within your community).

Technical questions: contact@ctiforecast.com. Online documentation: ctiforecast.com/en/docs and ctiforecast.com/en/integrations. The French terms of sale prevail in case of discrepancy.