CTI / FORECAST

POUR LES ÉQUIPES TECHNIQUES

Fiche technique et guide d'intégration

Données, API, TAXII 2.1, STIX 2.1, intégrations, sécurité et exploitation : la référence pour les équipes techniques.

DIFFUSABLE

Destinataires
RSSI, SOC, administrateurs, intégrateurs

Version
1.0 · 7 novembre 2026

Support
contact@ctiforecast.com

Sommaire

01 Présentation du service
02 Collecte et traitement des données
03 Modèle de données
04 Confiance et décroissance
05 Accès à l'API
06 Référence des points d'accès
07 TAXII 2.1 et STIX 2.1
08 Guides d'intégration
09 Sécurité et confidentialité
10 Disponibilité et support
11 Questions fréquentes

01 Présentation du service

CTI Forecast fournit un flux d'indicateurs de compromission (IOC) et des prévisions d'exploitation de vulnérabilités, accessibles par API REST, par un serveur TAXII 2.1, en bundles STIX 2.1 et en listes de blocage texte. Ce document décrit les données, les interfaces, les intégrations courantes, la sécurité et l'exploitation du service, pour les équipes qui le mettent en place.

CARACTÉRISTIQUE	VALEUR
Types d'indicateurs	`ip` (IPv4/IPv6), `domain`, `url`, `sha256`, `sha1`, `md5`, `cve`
Sources	339 sources de recherche (éditeurs, CERT, laboratoires) et flux curés (ESET malware-ioc, abuse.ch Feodo Tracker et SSL Blacklist)
Volume	Plus de 257 000 indicateurs publiés (novembre 2026)
Fraîcheur	Synchronisation toutes les 5 minutes (plans Pro et Business)
Enrichissement	Confiance 0-100, source et articles, ASN, opérateur et pays des IP, famille de malware si connue
Interfaces	API REST JSON (OpenAPI 3.1), TAXII 2.1, STIX 2.1, texte brut, CSV
Hébergement des données	France ; diffusion via Cloudflare
Spécification	`https://ctiforecast.com/openapi.json`

02 Collecte et traitement des données

1. **Collecte** : lecture continue des publications de recherche en sécurité ; extraction des candidats (IP, domaines, URL, hashes, CVE), y compris sous forme désamorcée (`hxxp` , `[.]`).
2. **Filtrage** : suppression des faux positifs connus :
   - domaines légitimes : grands services, messageries, et les 10 000 sites les plus visités (liste Tranco, mise à jour chaque semaine) ;
   - IP de CDN et de grands services ; plages non routées ; résolveurs publics ; numéros de version pris pour des IP ;
   - extensions de fichiers prises pour des domaines (`config.json`) ; domaines des sites sources eux-mêmes.
3. **Notation** : score de confiance selon le type de source, la corroboration, la répétition, le type de réseau (section 4).
4. **Croisement** avec les flux curés et, pour les CVE, avec EPSS (FIRST) et le catalogue KEV de la CISA.
5. **Publication** : seuls les indicateurs au-dessus des seuils sont servis ; leur confiance décroît avec le temps.

Le collecteur ne fait que lire des publications : il n'interagit jamais avec l'infrastructure des attaquants. Moins d'un candidat sur cinq passe les filtres.

03 Modèle de données

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

CHAMP	TYPE	DESCRIPTION
`value`	string	Valeur, non désamorcée dans l'API
`type`	string	`ip` , `domain` , `url` , `sha256` , `sha1` , `md5` , `cve`
`confidence`	entier 0-100	Confiance actuelle, après décroissance
`confidence_base`	entier 0-100	Confiance d'origine, avant décroissance
`severity`	entier ou null	Sévérité estimée par le collecteur
`first_seen` , `last_seen`	ISO 8601 (UTC)	Première et dernière observation
`mentions`	entier	Nombre d'observations
`source`	string	Source principale
`category` , `malware_family`	string ou null	Catégorie et famille, si connues
`asn` , `as_name` , `country`	IP uniquement	Système autonome, opérateur, pays (ISO 3166-1)
`references`	liste	Jusqu'à 3 sources (5 pour un lookup) : `url` , `source` , `seen_at` , et pour les flux curés `context` et `curated: true` . Vide en Free

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

CHAMP	DESCRIPTION
`signal`	`exploitee` (déjà au KEV), `imminente` , `a_surveiller` , `faible`
`forecast_score`	Rang 0-100 parmi les CVE suivies
`kev_probability_30d`	Probabilité estimée d'ajout au KEV sous 30 jours
`epss` , `epss_percentile` , `epss_date`	Données EPSS du jour
`in_kev` , `kev_date_added` , `kev_ransomware_use`	Statut dans le catalogue de la CISA
`mentions_7d` , `mentions_previous_7d` , `active_days_7d`	Dynamique des publications
`reasons`	Explication lisible du score (actuellement en français)

04 Confiance et décroissance

Le score de confiance (0-100) résume la fiabilité d'un indicateur. Pour les IP, il combine :

- le **type de source** : flux curé publié par l'éditeur (fort), laboratoire de recherche, média spécialisé, avis de sécurité (faible) ;
- la **corroboration** par plusieurs sources indépendantes ;
- la **répétition** des observations et la sévérité ;
- le **type de réseau** (ASN) : hébergeur VPS (hausse), cloud public (légère baisse) ; les IP de CDN et de grands services ne sont jamais publiées.

Décroissance

Sans nouvelle observation, la confiance diminue de moitié en **30 jours** pour les IP et les URL, et en **90 jours** pour les domaines, après 7 jours de grâce. Les empreintes de fichiers et les CVE ne décroissent pas. La valeur d'origine reste disponible dans `confidence_base`.

Seuils recommandés

USAGE	MIN_CONFIDENCE CONSEILLÉ
Blocage automatique (pare-feu, DNS filtrant)	≥ 70 (valeur par défaut des listes de blocage)
Alerte dans un SIEM	≥ 50
Enrichissement, chasse aux menaces	≥ 40 (minimum servi pour les IP)

> **Bonne pratique**
> Démarrer en mode alerte (sans blocage) pendant une à deux semaines, vérifier les correspondances avec vos journaux, puis activer le blocage. Gardez une liste d'exceptions locale pour vos partenaires.

05 Accès à l'API

Généralités

ÉLÉMENT	VALEUR
URL de base	`https://ctiforecast.com`
Format	JSON UTF-8 ; dates ISO 8601 en UTC
Authentification	En-tête `X-API-Key: <clé>` (recommandé), `Authorization: Bearer <clé>`, Basic (mot de passe = clé, pour TAXII), ou `?key=` pour les outils qui ne gèrent pas les en-têtes
Clés	Créées dans « Mon compte », affichées une seule fois, révocables ; plusieurs clés possibles (une par outil)
Quotas	Free 100, Pro 10 000, Business 100 000 requêtes par jour ; remise à zéro à minuit UTC
En-têtes de quota	`X-RateLimit-Limit`, `X-RateLimit-Remaining`
Langue des messages	Selon `Accept-Language` (`fr` ou `en`)

Codes de réponse

CODE	SIGNIFICATION
200	Succès
400	Paramètre invalide (message dans `error`)
401	Clé manquante, invalide ou révoquée
403	Fonction ou type non inclus dans la formule
429	Quota journalier atteint

Pagination et collecte incrémentale

`/v1/iocs` renvoie les indicateurs du plus récent au plus ancien. Pour la page suivante, passez la valeur `next_until` en paramètre `until`. Pour une collecte incrémentale, mémorisez l'heure de votre dernière collecte et passez-la en `since`.

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

06 Référence des points d'accès

ROUTE	PARAMÈTRES	RÉPONSE	FORMULE
`GET /v1/iocs`	type, since, until, min_confidence, limit (max 100 / 1 000 / 5 000)	`count` , `next_until` , `delayed_hours` , `data[]`	Toutes
`GET /v1/lookup`	value (obligatoire)	`found` , `matches[]`	Toutes
`GET /v1/stats`	—	Formule, volumes, quota du jour	Toutes
`GET /v1/blocklist.txt`	type (ip, domain, url, sha256, sha1, md5), days (1-365, 30), min_confidence (70)	Texte, une valeur par ligne	Types de la formule
`GET /v1/trending`	type, status (nouveau, en_hausse, stable, en_baisse), min_confidence, limit	Indicateurs en accélération (7 j contre 7 j)	Free : top 10
`GET /v1/forecast`	signal, min_score, limit	CVE classées par probabilité	Free : top 10
`GET /v1/cve/{{id}}`	identifiant CVE	Fiche complète	Toutes
`GET /v1/stix`	comme /v1/iocs	Bundle STIX 2.1	Pro, Business
`GET /v1/export`	comme /v1/iocs + format (csv, json)	Jusqu'à 500 000 lignes	Business

Exemple de réponse (`/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"}]}]}
```


Valeurs d'illustration. La spécification complète, avec tous les schémas, est disponible dans `/openapi.json` .

07 TAXII 2.1 et STIX 2.1

Serveur TAXII (lecture seule, Pro et Business)

ÉLÉMENT	VALEUR
Découverte	`https://ctiforecast.com/taxii2/`
Racine d'API	`https://ctiforecast.com/taxii2/api/`
Authentification	Basic : utilisateur au choix, mot de passe = clé API
Filtres	`added_after` , `match[type]` , `limit` ; pagination par `next`

COLLECTION	IDENTIFIANT	CONTENU
IP malveillantes	`77653c02-ccd7-55e5-8db8-85d421cfba7c`	IPv4 / IPv6
Domaines et URL malveillants	`6d85c187-7ce5-561a-9cb0-d820a89fd099`	domain, url
Fichiers malveillants	`60ef1a80-e85a-56e8-84b6-f6e51e8d3fb6`	sha256, sha1, md5
Vulnérabilités	`00ae1b11-d2b2-550f-91d2-39efc6c29dd7`	CVE

Correspondance STIX 2.1

- Chaque IOC devient un objet `indicator` (`pattern_type: stix` , `indicator_types: malicious-activity`) ; les CVE deviennent des objets `vulnerability` .
- Motifs : `[ipv4-addr:value = '…']` , `[ipv6-addr:value = '…']` , `[domain-name:value = '…']` , `[url:value = '…']` , `[file:hashes.'SHA-256' = '…']` .
- `confidence` reprend le score ; `valid_until` suit la décroissance ; marquage **TLP:GREEN** ; articles sources en `external_references` .
- Identifiants stables : réimporter met à jour les objets existants au lieu de créer des doublons.
- Conformité vérifiée avec les bibliothèques officielles OASIS (`stix2` , `taxii2-client`).

08 Guides d'intégration

Dans les exemples, remplacez `VOTRE_CLE` par une clé dédiée à l'outil. Les URL contenant la clé donnent accès à votre compte : ne les publiez pas.

pfSense / OPNsense

Firewall → Aliases → URLs (OPNsense : **Firewall → Aliases**, type URL Table), nom `CTI_FORECAST_IP`, mise à jour quotidienne, URL :

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

Créez ensuite une règle **Block** sur l'interface WAN (entrée) et LAN (sortie) avec cet alias.

Wazuh (liste CDB)

```
curl -fsS "https://ctiforecast.com/v1/blocklist.txt?type=ip&days=30&key=VOTRE_CLE" \
  | 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
```

Déclarez `<list>etc/lists/cti-forecast-ip</list>` dans `ossec.conf` et ajoutez une règle `<list field="srcip" lookup="address_match_key">`.

OpenCTI

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

Microsoft Sentinel

Content hub → solution *Threat Intelligence* → connecteur *Threat Intelligence - TAXII* : racine `https://ctiforecast.com/taxii2/api/`, identifiant de collection (section 7), utilisateur `client`, mot de passe = clé, interrogation toutes les heures.

MISP

Sync Actions → Feeds → Add Feed, format *Freetext Parsed Feed*, un flux par type :

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

Splunk

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

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

Autres outils

Elastic, QRadar, TheHive, scripts Python, n8n : toute solution capable d'une requête HTTP peut utiliser l'API JSON. Générez un client à partir de `/openapi.json` avec *openapi-generator*.

09 Sécurité et confidentialité

DOMAINE	MESURE
Transport	HTTPS uniquement, TLS 1.2 minimum, HSTS
Clés API	Stockées sous forme d'empreinte irréversible ; affichées une seule fois ; révocables à tout moment
Comptes	Mots de passe hachés ; double authentification (TOTP) disponible ; limitation des tentatives
Valeurs interrogées	**Jamais conservées** : ni en base, ni dans les journaux (les journaux n'enregistrent pas les paramètres d'URL)
Données conservées	Compte (email, société), nombre de requêtes par jour, facturation (Stripe)
Infrastructure	Aucun port entrant exposé sur Internet ; accès via le réseau Cloudflare
Sauvegardes	Chiffrées (AES-256) avant envoi, hébergées en France, immuables pendant 30 jours
RGPD	DPA (article 28) publié : ctiforecast.com/dpa ; version signée sur demande
Divulgation responsable	security@ctiforecast.com ; politique sur ctiforecast.com/securite ; `/.well-known/security.txt`

Recommandations

- Utilisez une clé par outil, pour pouvoir en révoquer une sans couper les autres.
- Préférez l'en-tête `X-API-Key` au paramètre `?key=` quand l'outil le permet.
- Activez la double authentification sur le compte qui gère les clés.

10 Disponibilité et support

ÉLÉMENT	ENGAGEMENT ACTUEL
Fraîcheur des données	Synchronisation toutes les 5 minutes ; flux curés toutes les 6 heures ; prévisions chaque jour
Surveillance	Contrôle automatique toutes les 5 minutes (synchronisation, collecte, prévisions, sauvegardes, disque)
Page de statut publique	stats.uptimerobot.com/J8ZkzyVqvK
Support	contact@ctiforecast.com, réponse sous un jour ouvré
SLA contractuel	Non proposé à ce jour ; étude au cas par cas pour les offres sur devis
Évolutions	Annoncées sur ctiforecast.com/nouveautes, à l'avance si elles modifient l'API

Conseils de robustesse

- Interrogez les listes de blocage au plus toutes les heures : elles ne changent pas plus vite que la synchronisation.
- En cas d'erreur réseau ou de code 5xx, conservez la dernière liste valide et réessayez plus tard avec un délai croissant.
- Surveillez `X-RateLimit-Remaining` pour ne pas atteindre le quota.

11 Questions fréquentes

QUESTION	RÉPONSE
Les valeurs sont-elles désamorcées ?	Non dans l'API et les listes (pour être utilisables par vos outils). Elles le sont sur le site web (`exemple[.]com`).
Pourquoi une IP a-t-elle disparu de la liste ?	Sa confiance est passée sous le seuil par décroissance, ou elle a été reconnue comme légitime (CDN, grand service).
Puis-je signaler un faux positif ?	Oui : contact@ctiforecast.com, avec la valeur et le contexte. Il est traité et peut améliorer les filtres pour tous.
Quelle différence entre Free et Pro ?	Free : CVE et SHA-256 seulement, 24 h de décalage, sans sources. Pro : tous les types, temps réel, sources, TAXII et STIX.
Puis-je tester sans m'inscrire ?	Oui : échantillon CSV sur ctiforecast.com/echantillon. L'essai Pro de 14 jours est sans carte bancaire.
Les données peuvent-elles être redistribuées ?	Usage interne à votre organisation. Toute redistribution hors de celle-ci (par exemple un MSSP vers ses clients) demande un accord écrit, prévu dans les offres sur devis. Voir les CGV.
Quel est le marquage TLP ?	Les indicateurs STIX sont marqués TLP:GREEN (partage possible au sein de votre communauté).

Pour toute question technique : contact@ctiforecast.com. Documentation en ligne : ctiforecast.com/docs et ctiforecast.com/integrations.