

ThreatQuotient

A Securonix Company



CrowdSec Threat Intelligence CDF

Version 2.0.0

September 14, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



ThreatQ Supported

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
CrowdSec Threat Intelligence Indicators Parameters	9
CrowdSec Smoke CTI Parameters	10
ThreatQ Mapping	11
CrowdSec Threat Intelligence Indicators	11
CrowdSec Smoke CTI	13
Shared Mapping	14
Average Feed Run	16
CrowdSec Threat Intelligence Indicators	16
CrowdSec Smoke CTI	16
Change Log	17

Warning and Disclaimer

ThreatQuotient, Inc. provides this document "as is", without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein.

ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com

Support Web: <https://ts.securonix.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version 2.0.0

Compatible with ThreatQ Versions $\geq 5.25.0$

Support Tier ThreatQ Supported

Introduction

The CrowdSec Threat Intelligence integration allows a user to ingest the latest IPs belonging to the CrowdSec community-blocklist.

The integration provides the following feeds:

- **CrowdSec Threat Intelligence Indicators** - ingests the latest IPs belonging to the CrowdSec community-blocklist.
- **CrowdSec Smoke CTI** - ingests IP intelligence matching a user-supplied CrowdSec Lucene query.

The integration ingests the following system object types:

- Attack Patterns
- Indicators
 - Indicator Attributes
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A CrowdSec CTI API key with access to the selected endpoint is required.
Programmatic access to Lucene search may require an Advanced CTI plan.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

CrowdSec Threat Intelligence Indicators Parameters

PARAMETER	DESCRIPTION
API Key	Enter your CrowdSec API Key.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Ingest CVE Data as	Select whether to ingest CVEs as indicators of vulnerabilities. The Vulnerabilities option is selected by default.

CrowdSec Smoke CTI Parameters

PARAMETER	DESCRIPTION
API Key	Enter your CrowdSec API Key.
Search Query	Enter the CrowdSec Lucene query used to identify the IP addresses to ingest.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Ingest CVE Data as	Select whether to ingest CVEs as indicators of vulnerabilities. The Vulnerabilities option is selected by default.

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

CrowdSec Threat Intelligence Indicators

The CrowdSec Threat Intelligence Indicators feed retrieves and ingests the latest IPs belonging to the CrowdSec community-blocklist.



Duration is calculated in minutes and represents the last duration minutes for which the data are returned.

GET <https://cti.api.crowdsec.net/v2/fire?page=1&since={duration}>

Sample Response (truncated):

```
{
  "ip": "216.73.161.91",
  "ip_range": "216.73.160.0/22",
  "as_name": "Ipxo Limited",
  "as_num": 206092,
  "reputation": "malicious",
  "location": {
    "country": "US",
    "city": "New York"
  },
  "behaviors": [
    {
      "name": "http:exploit",
      "label": "HTTP Exploit"
    }
  ],
  "history": {
    "first_seen": "2022-08-24T12:15:00+00:00",
    "last_seen": "2024-02-03T11:00:00+00:00"
  },
  "attack_details": [
    {
      "name": "crowdsecurity/http-sqli-probbing-detection",
      "label": "SQL Injection Attempt"
    }
  ],
  "state": "validated",
}
```

```
"background_noise": "medium",
"mitre_techniques": [
  {
    "name": "T1595",
    "label": "Active Scanning"
  }
],
"cves": [
  "CVE-2023-49103"
],
"scores": {
  "overall": {
    "aggressiveness": 5,
    "threat": 1,
    "trust": 5,
    "anomaly": 1,
    "total": 4
  }
}
}
```

CrowdSec Smoke CTI

The CrowdSec Smoke CIT feed retrieves and ingests CrowdSec IP intelligence that matches a user-supplied Lucene query.

```
GET https://cti.api.crowdsec.net/v2/smoke/search?query={query}&page=1&since={duration}
```

The feed calculates duration in minutes from the ThreatQ run interval and follows CrowdSec's `_links.next` URL until all pages are processed. CrowdSec requires Boolean operators such as `AND` and `OR` to be uppercase.

Example queries:

- `classifications.classifications.name:"profile:web_hosting" AND (reputation:malicious OR reputation:suspicious)`
- `classifications.classifications.name:/.*:mirai/ OR classifications.classifications.name:/.*:mozi/`

The Smoke feed uses the shared CrowdSec mapping above, excluding the Fire-only state and expiration attributes.

Shared Mapping

ThreatQuotient provides the following default mapping for both feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	NOTES
items[].ip	Indicator Value	IP Address	items[].history.fir st_seen	
items[].as_name	Indicator Attribute	Name	items[].history.fir st_seen	Updates at ingestion
items[].as_num	Indicator Attribute	ASN	items[].history.fir st_seen	Updates at ingestion
items[].reputation	Indicator Attribute	Reputation	items[].history.fir st_seen	Updates at ingestion
items[].confidence	Indicator Attribute	Confidence	items[].history.fir st_seen	Updates at ingestion
items[].ip_range	Indicator Attribute	IP Range	items[].history.fir st_seen	Updates at ingestion
items[].ip_range_score	Indicator Attribute	IP Range Score	items[].history.fir st_seen	Updates at ingestion
items[].ip_range_24	Indicator Attribute	IP Range /24	items[].history.fir st_seen	Updates at ingestion
items[].ip_range_24_reputation	Indicator Attribute	IP Range /24 Reputation	items[].history.fir st_seen	Updates at ingestion
items[].ip_range_24_score	Indicator Attribute	IP Range /24 Score	items[].history.fir st_seen	Updates at ingestion
items[].location.country	Indicator Attribute	Country Code	items[].history.fir st_seen	Updates at ingestion
items[].location.city	Indicator Attribute	City	items[].history.fir st_seen	Updates at ingestion
items[].location.latitude	Indicator Attribute	Latitude	items[].history.fir st_seen	Updates at ingestion
items[].location.longitude	Indicator Attribute	Longitude	items[].history.fir st_seen	Updates at ingestion
items[].reverse_dns	Indicator Attribute	rDNS	items[].history.fir st_seen	Updates at ingestion
items[].history.last_seen	Indicator Attribute	Last seen	items[].history.fir st_seen	Updates at ingestion
items[].state	Indicator Attribute	Indicator State	items[].history.fir st_seen	Fire endpoint only
items[].target_countries	Indicator Attribute	Target Country Code	items[].history.fir st_seen	Country codes are joined into one value
items[].target_countries	Indicator Attribute	Target Country Distribution	items[].history.fir st_seen	Preserves CrowdSec's per-country percentages
items[].expiration	Indicator Attribute	Expiration date	items[].history.fir st_seen	Fire endpoint only

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	NOTES
items[].scores.overall.aggressiveness	Indicator Attribute	Aggressiveness Score	items[].history.first_seen	Updates at ingestion
items[].scores.overall.threat	Indicator Attribute	Threat Score	items[].history.first_seen	Updates at ingestion
items[].scores.overall.trust	Indicator Attribute	Trust Score	items[].history.first_seen	Updates at ingestion
items[].scores.overall.anomaly	Indicator Attribute	Anomaly Score	items[].history.first_seen	Updates at ingestion
items[].scores.overall.total	Indicator Attribute	Overall Score	items[].history.first_seen	Updates at ingestion
items[].scores.last_day.total	Indicator Attribute	Last Day Score	items[].history.first_seen	Updates at ingestion
items[].scores.last_week.total	Indicator Attribute	Last Week Score	items[].history.first_seen	Updates at ingestion
items[].scores.last_month.total	Indicator Attribute	Last Month Score	items[].history.first_seen	Updates at ingestion
items[].background_noise	Indicator Attribute	Noise	items[].history.first_seen	Updates at ingestion
items[].background_noise_score	Indicator Attribute	Background Noise Score	items[].history.first_seen	Updates at ingestion
items[].proxy_or_vpn	Indicator Attribute	Proxy or VPN	items[].history.first_seen	Mapped when supplied by CrowdSec
items[].behaviors[].name	Indicator Attribute	CrowdSec Behavior	items[].history.first_seen	Multi-value
items[].classifications.classifications[].name	Indicator Attribute	CrowdSec Classification	items[].history.first_seen	Multi-value
items[].classifications.false_positives[].name	Indicator Attribute	CrowdSec False Positive	items[].history.first_seen	Multi-value
items[].attack_details[].name	Indicator Attribute	CrowdSec Attack Detail	items[].history.first_seen	Multi-value
items[].references[].name	Indicator Attribute	CrowdSec Reference	items[].history.first_seen	Multi-value
items[].cves	Related Vulnerabilities / Indicators	CVE	items[].history.first_seen	Controlled by Ingest CVEs as
items[].mitre_techniques	Related Attack Patterns	MITRE ATT&CK technique	items[].history.first_seen	Links to existing ThreatQ Attack Patterns

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

CrowdSec Threat Intelligence Indicators

METRIC	RESULT
Run Time	8 minute
Indicators	10,232
Indicator Attributes	92,799
Vulnerabilities	32
Attack Pattern	1

CrowdSec Smoke CTI

METRIC	RESULT
Run Time	1 minute
Indicators	451
Indicator Attributes	19,043

Change Log

- **Version 2.0.0**
 - Added the **CrowdSec Smoke CTI** feed, enabling customers to ingest CrowdSec Smoke threat intelligence into ThreatQ.
 - Expanded CrowdSec CTI data mappings and standardized shared processing across CrowdSec feeds to provide more complete and consistent data ingestion.
- **Version 1.0.1**
 - Added `User-Agent` to the request.
- **Version 1.0.0**
 - Initial release