

ThreatQuotient



CrowdSec CDF User Guide

Version 1.0.0

February 13, 2024

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

ThreatQ Mapping..... 10

 CrowdSec Threat Intelligence Indicators 10

Average Feed Run..... 15

Change Log 16

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 © 2024 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: support@threatq.com

Support Web: <https://support.threatq.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 1.0.0

**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 feed:

- **CrowdSec Threat Intelligence Indicators** - ingests the latest IPs belonging to the CrowdSec community-blocklist.

The integration ingests the following system object types:

- Attack Patterns
- Indicators
 - Indicator Attributes
- Vulnerabilities

Prerequisites

A CrowdSec API Key is required by the integration.

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:

PARAMETER	DESCRIPTION
API Key	Enter your CrowdSec API Key.
Save CVE Data as	Select whether to ingest CVEs as indicators of vulnerabilities. The Vulnerabilities option is selected by default.

< CrowdSec Threat Intelligence Indicators



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

API Key

Save CVE Data As **Vulnerabilities**

ThreatQuotient maps CVE data as CVE Vulnerabilities by default.

Set indicator status to... **Active**

Run Frequency **Every 24 Hours**

Next scheduled run: 2024-02-13 05:23am (-05:00)

☒ Send a notification when this feed encounters issues.

☒ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. 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:

```
{
  "ip_range_score": 5,
  "ip": "216.73.161.91",
  "ip_range": "216.73.160.0/22",
  "as_name": "Ipxo Limited",
  "as_num": 206092,
  "ip_range_24": "216.73.161.0/24",
  "ip_range_24_reputation": "malicious",
  "ip_range_24_score": 5,
  "reputation": "malicious",
  "location": {
    "country": "US",
    "city": "New York",
    "latitude": 40.7157,
    "longitude": -74.0
  },
  "reverse_dns": null,
  "behaviors": [
    {
      "name": "http:exploit",
      "label": "HTTP Exploit",
      "description": "IP has been reported for attempting to exploit a vulnerability in a web application.",
      "references": []
    },
    {
      "name": "http:scan",
      "label": "HTTP Scan",
      "description": "IP has been reported for performing actions related to HTTP vulnerability scanning and discovery.",
      "references": []
    }
  ]
}
```

```

        "name": "http:bruteforce",
        "label": "HTTP Bruteforce",
        "description": "IP has been reported for performing a HTTP
brute force attack (either generic HTTP probing or applicative related brute
force).",
        "references": []
    },
],
"history": {
    "first_seen": "2022-08-24T12:15:00+00:00",
    "last_seen": "2024-02-03T11:00:00+00:00",
    "full_age": 529,
    "days_age": 528
},
"classifications": {
    "false_positives": [],
    "classifications": [
        {
            "name": "community-blocklist",
            "label": "CrowdSec Community Blocklist",
            "description": "IP belongs to the CrowdSec Community
Blocklist"
        }
    ]
},
"attack_details": [
    {
        "name": "crowdsecurity/http-sqli-probbing-detection",
        "label": "SQL Injection Attempt",
        "description": "A scenario that detects SQL injection
probbing with minimal false positives",
        "references": []
    },
    {
        "name": "crowdsecurity/http-probbing",
        "label": "HTTP Probbing",
        "description": "Detect site scanning/probbing from a single
ip",
        "references": []
    },
    {
        "name": "crowdsecurity/http-bad-user-agent",
        "label": "detection of bad user-agents",
        "description": "Detect bad user-agents",
        "references": []
    },
    {
        "name": "crowdsecurity/http-backdoors-attempts",
        "label": "scanning for backdoors",
        "description": "Detect attempt to common backdoors",

```

```

        "references": []
      },
      {
        "name": "crowdsecurity/CVE-2023-49103",
        "label": "owncloud CVE-2023-49103",
        "description": "Detect owncloud CVE-2023-49103 exploitation
attempts",
        "references": []
      }
    ],
    "state": "validated",
    "expiration": "2024-02-12T07:48:32.269000",
    "target_countries": {
      "AU": 11,
      "BE": 3,
      "BG": 1,
      "BR": 4,
      "CA": 8,
      "CH": 5,
      "CL": 0,
      "CY": 0,
      "CZ": 0,
      "DE": 61
    },
    "background_noise_score": 7,
    "background_noise": "medium",
    "mitre_techniques": [
      {
        "name": "T1595",
        "label": "Active Scanning",
        "description": "Adversaries may execute active
reconnaissance scans to gather information that can be used during targeting.",
        "references": []
      },
      {
        "name": "T1110",
        "label": "Brute Force",
        "description": "Adversaries may use brute force techniques
to gain access to accounts when passwords are unknown or when password hashes
are obtained.",
        "references": []
      },
      {
        "name": "T1589",
        "label": "Gather Victim Identity Information",
        "description": "Adversaries may gather information about
the victim's identity that can be used during targeting.",
        "references": []
      }
    ]
  }

```

```

        "name": "T1190",
        "label": "Exploit Public-Facing Application",
        "description": "Adversaries may attempt to exploit a
weakness in an Internet-facing host or system to initially access a network.",
        "references": []
    }
],
"cves": [
    "CVE-2023-49103"
],
"scores": {
    "overall": {
        "aggressiveness": 5,
        "threat": 1,
        "trust": 5,
        "anomaly": 1,
        "total": 4
    },
    "last_day": {
        "aggressiveness": 0,
        "threat": 0,
        "trust": 0,
        "anomaly": 1,
        "total": 0
    },
    "last_week": {
        "aggressiveness": 5,
        "threat": 1,
        "trust": 5,
        "anomaly": 1,
        "total": 4
    },
    "last_month": {
        "aggressiveness": 3,
        "threat": 1,
        "trust": 5,
        "anomaly": 1,
        "total": 3
    }
},
"references": []
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
items[].ip	Indicator Value	N/A	items[].history.first_seen	216.73.161.91	N/A
items[].as_name	Indicator Attribute	Name	items[].history.first_seen	pxo Limited	N/A
items[].reputation	Indicator Attribute	Reputation	items[].history.first_seen	Malicious	Updates at ingestion
items[].location.country	Indicator Attribute	Country Code	items[].history.first_seen	US	
items[].history.last_seen	Indicator Attribute	Last seen	items[].history.first_seen	2024-02-03T11:00:00+00:00	Updates at ingestion
items[].state	Indicator Attribute	Indicator State	items[].history.first_seen	Validated	
items[].target_countries	Indicator Attribute	Target Country Code	items[].history.first_seen	AU, BE, BG, BR, CA, CH, CL, VY, CZ, DE	Updates at ingestion
items[].expiration	Indicator Attribute	Expiration date	items[].history.first_seen	2024-02-12T07:48:32.269000	Updates at ingestion
items[].scores.overall.threat	Indicator Attribute	Threat Score	items[].history.first_seen	1	Updates at ingestion
items[].background_noise	Indicator Attribute	Noise	items[].history.first_seen	Medium	Updates at ingestion
items[].cves	Related Vulnerabilities/ Indicators	N/A	items[].history.first_seen	CVE-2023-49103	
items[].mitre_techniques	Related Attack Patterns	N/A	items[].history.first_seen	T1589	Linked to already existing TQ MITRE Attack Pattern

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.

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

Change Log

- Version 1.0.0
 - Initial release