

# ThreatQuotient



## Cybercrime Tracker Guide

**Version 1.0.1**

July 07, 2021

**ThreatQuotient**

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

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](http://support.threatq.com)

Phone: 703.574.9893

# 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 © 2021 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.

# Contents

Versioning..... 4

Introduction..... 5

Installation ..... 6

Configuration..... 7

ThreatQ Mapping..... 8

    CyberCrime Tracker ..... 8

Average Feed Run ..... 10

Change Log..... 11

# Versioning

- Current integration version: 1.0.1
- Supported on ThreatQ versions  $\geq$  4.3.0

# Introduction

CyberCrime Tracker is an open source intelligence source found at <https://cybercrime-tracker.net>.

# 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 **Cybercrime Tracker** feed 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 **OSINT** 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. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

# ThreatQ Mapping

## CyberCrime Tracker

GET `http://cybercrime-tracker.net/all.php`

This endpoint returns text containing a newline delimited list of URLs

```
www.tepevizyon.com.tr/xx/Panel/PvqDq929BSx_A_D_M1n_a.php
95.181.155.150/login.php
viihaiha.com/.ill/news/school/boy/choo/PvqDq929BSx_A_D_M1n_a.php
194.58.103.2/main/login.php
185.215.113.53/bPwsAq2/login.php
manvim.co/fc7/PvqDq929BSx_A_D_M1n_a.php
manvim.co/os/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fc5/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fc6/PvqDq929BSx_A_D_M1n_a.php
manvim.co/bo/PvqDq929BSx_A_D_M1n_a.php
mxrz.xyz/tker3/w2/PvqDq929BSx_A_D_M1n_a.php
sspmoct.xyz/tkrr/T1/w2/PvqDq929BSx_A_D_M1n_a.php
es02.xyz/w2/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fd6/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fd4/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fd5/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fd3/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fd1/PvqDq929BSx_A_D_M1n_a.php
manvim.co/fd2/PvqDq929BSx_A_D_M1n_a.php
gepardmain.com/admin/
gjusvoqmkddfahvoccsx.com/figrab/
gjusvoqmkddfahvoccsx.com/ebayadmin/
wenolira.top/bofaadmin/
gjusvoqmkddfahvoccsx.com/amzccadvadmin/
asilcosmetics.ru/modules/mod_articles/mod_articles.php
security-apple-manage.com/
test.danrinok.ru/administrator/components.php
allonston.com/modules/mod_fxprev/helper.php
приволжское-мпо-жкх.рф/modules/mod_ariimageslidorsa/mod_ariimageslidorsa.php
10words.radiofreepirate.org/sites/default/files/_hash.php
www.tsqprivatskver.ru/index.php
iryston.com/index.php
iwebtechexpert.com/blog/wp-admin/js/9givn.php
adkpower.in/class.php
esselfire.com/templates/default/css/popup.php
caudan-vous-accueille.com/images/gmapfp/hsfgdyfy.php?pass=kod3
bsc.org.np/
178.20.47.174/po02jewaf092/admin/login.php
ahcteam.tech/login.php
212.192.241.97/~botboyz/login.php
51.222.56.151/tsc/login.php
www.chika1995.xyz/enfix/chik/ad/Panel/five/PvqDq929BSx_A_D_M1n_a.php
aaastyloff.xyz/cheque/hen/ad/Panel/five/PvqDq929BSx_A_D_M1n_a.php
212.192.241.220/login.php
212.192.241.91/login.php
www.mibbpersonales.com/tacabamba/index.php
```

```
ctp1.xyz/w2/PvqDq929BSx_A_D_M1n_a.php
matix.cf/panel/login.php
greenbazaar.xyz/blac/panel/five/PvqDq929BSx_A_D_M1n_a.php
lushbb.xyz/sngtt/w2/PvqDq929BSx_A_D_M1n_a.php
...
```

ThreatQ provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY  | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                                                     | NOTES |
|----------------|-----------------|--------------------------------------|----------------|--------------------------------------------------------------|-------|
| 0              | Indicator.Value | URL                                  | N/A            | www.tepevizyon.com.tr/xx/Panel/<br>PvqDq929BSx_A_D_M1n_a.php | N/A   |

# 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             | 5m     |
| Indicators           | 22,500 |
| Indicator Attributes | 4,814  |
| Adversaries          | 0      |
| Adversary Attributes | 0      |

# Change Log

- **Version 1.0.1**
  - Addressed issue that prevented objects from being ingested
- **Version 1.0.0**
  - Initial Release