ThreatQuotient

PhishStats CDF User Guide

Version 1.0.0

November 29, 2023

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

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 **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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The PhishStats CDF is an open-source feed that ingests phishing URLS that have been reported to PhishStats. The feed automatically ingests the URLs, IPs, and relevant context into ThreatQ.

The integration provides the following feed:

- **PhishStats** - ingests the latest phishing URLs reported to PhishStats.

The integration ingests URL and IP type indicators along with relevant context.

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:

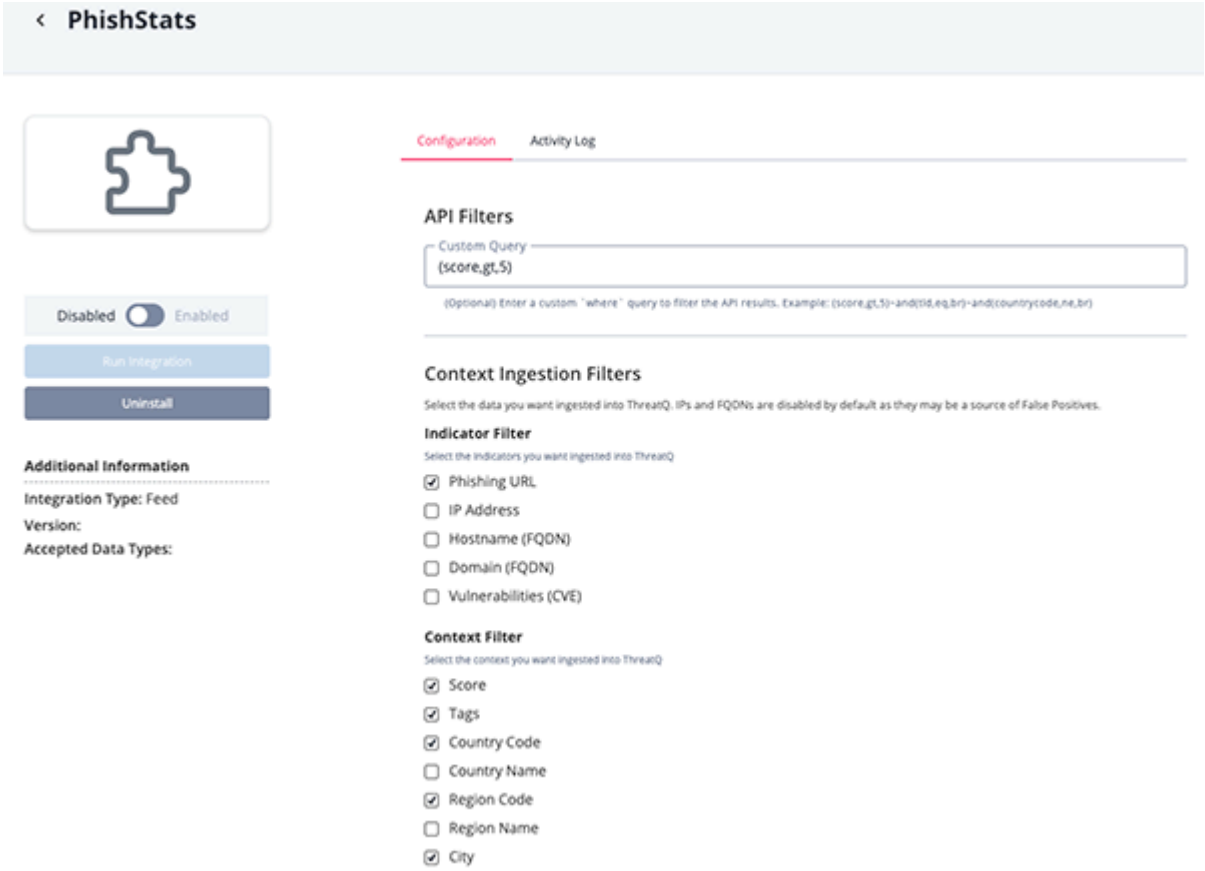
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
Custom Query	Optional - Enter a custom `where` query to filter the API results. **Example**: `(score,gt,5)~and(tld,eq,br)~and(countrycode,ne,br)`
Indicator Filter	Select the indicator types to ingest. Options include: ◦ Phishing URL (default) > If this option is not enabled, ingested indicators will not be related. ◦ IP Address ◦ Hostname (FQDN) ◦ Domain (FQDN) ◦ Vulnerabilities (CVE)
Context Filter	Select the context to ingest. Options include: ◦ Score (default) ◦ Tags (default) ◦ Country Code (default) ◦ Country Name ◦ ASN ◦ TLD ◦ ISP ◦ Domain Registered Days Ago (default)

PARAMETER	DESCRIPTION
	◦ Region Code (default) ◦ Region Name ◦ City (default) ◦ Zip Code ◦ Latitude ◦ Longitude ◦ HTTP Server ◦ Ports ◦ Abuse Contact Email ◦ Operating System ◦ Page Title
Ignore Domains with Alexa Rank	If enabled, domains and IPs that are Alexa ranked will not be ingested into the ThreatQ platform. This option is enabled by default.
Ignore Hostnames with Alexa Rank	If enabled, hostnames and IPs that are Alexa ranked will not be ingested into the ThreatQ platform. This option is enabled by default.
Ingest CVEs As	Select the object type to ingest CVEs as. Options include: ◦ Indicators (CVE) ◦ Vulnerabilities (default)



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

PhishStats

The PhishStats feed ingests phishing URLs into ThreatQ, along with any related context, CVEs, FQDNs, and IP addresses.

`GET https://phishstats.info:2096/api/phishing`

Sample Response:


```
[
  {
    "id": 9989504,
    "url": "https://business-meta-support-id867469.2254216.com/?
content_id=m0QTpkB3B22HWYc/",
    "ip": "104.21.45.160",
    "countrycode": "US",
    "countryname": "United States",
    "regioncode": "",
    "regionname": "",
    "city": "",
    "zipcode": "",
    "latitude": "37.7510",
    "longitude": "-97.8220",
    "asn": "AS13335",
    "bgp": "104.16.0.0/12",
    "isp": "CLOUDFLARENET, US",
    "title": "Meta",
    "date": "2023-06-20T14:47:20.000Z",
    "date_update": "2023-06-20T15:53:19.000Z",
    "hash": "044a09f39c51c70d3e41d9b639e6dd68f1a6cee7aa3fd2387943c67459ac76f3",
    "score": 6,
    "host": "business-meta-support-id867469.2254216.com",
    "domain": "2254216.com",
    "tld": "com",
    "domain_registered_n_days_ago": 5,
    "screenshot": null,
    "abuse_contact": "abuse@business-meta-support-id867469.2254216.com
abuse@2254216.com",
    "ssl_issuer": null,
    "ssl_subject": null,
    "alexa_rank_host": null,
    "alexa_rank_domain": null,
    "n_times_seen_ip": 2,
    "n_times_seen_host": 1,
    "n_times_seen_domain": 1,
    "http_code": 403,
```

```
    "http_server": null,
    "google_safebrowsing": null,
    "virus_total": "Yes",
    "abuse_ch_malware": "No",
    "threat_crowd": null,
    "threat_crowd_subdomain_count": null,
    "threat_crowd_votes": null,
    "vulns": "CVE-2016-20012, CVE-2017-15906, CVE-2018-15473, CVE-2018-15919",
    "ports": "80, 443, 2053, 2082, 2087, 2095, 8080, 8443, 8880",
    "os": null,
    "tags": "cdn",
    "technology": null,
    "page_text": null
  }
]
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.url`	Indicator.Value	URL	`.date`	`https://business-meta-support-id867469.2254216.com/...`	If user config `Indicator Filter` contains `Phishing URL`
`.ip`	Related Indicator.Value	IP Address, IPv6 Address	`.date`	`104.21.45.160`	If user config `Indicator Filter` contains `IP Address`
`.domain`	Related Indicator.Value	FQDN	`.date`	`2254216.com`	If user config `Indicator Filter` contains `Domain (FQDN)`
`.host`	Related Indicator.Value	FQDN	`.date`	`business-meta-support-id867469.2254216.com`	If user config `Indicator Filter` contains `Hostname (FQDN)`
`.vulns`	Related Indicator/ Vulnerability.Value	CVE	`.date`	`CVE-2016-20012`	Split by comma. If user config `Indicator Filter` contains `Vulnerabilities (CVE)`
`.tags`	Indicator.Tag	N/A	`.date`	`cdn`	Split by comma. If user config `Context Filter` contains `Tags`
`.ports`	Indicator.Attribute	Port	`.date`	`80, 443, 2053, 2082, 2087, 2095, 8080, 8443, 8880`	If user config `Context Filter` contains `Ports`
`.abuse_contact`	Indicator.Attribute	Abuse Contact	`.date`	`abuse@business-meta-support-id867469.2254216.com abuse@2254216.com`	Split by space. If user config `Context Filter` contains `Abuse Contact Email`
`.score`	Indicator.Attribute	Score	`.date`	`6`	Updated if already exists. If user config `Context Filter` contains `Score`
`.title`	Indicator.Attribute	Site Title	`.date`	`Meta`	If user config `Context Filter` contains `Site Title`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.countrycode`	Indicator.Attribute	Country Code	`.date`	`US`	If user config `Context Filter` contains `Country Code`
`.countryname`	Indicator.Attribute	Country	`.date`	`United States`	If user config `Context Filter` contains `Country Name`
`.regioncode`	Indicator.Attribute	Region Code	`.date`	N/A	If user config `Context Filter` contains `Region Code`
`.regionname`	Indicator.Attribute	Region	`.date`	N/A	If user config `Context Filter` contains `Region Name`
`.city`	Indicator.Attribute	City	`.date`	N/A	If user config `Context Filter` contains `City`
`.zipcode`	Indicator.Attribute	Zip Code	`.date`	N/A	If user config `Context Filter` contains `Zip Code`
`.latitude`	Indicator.Attribute	Latitude	`.date`	`37.7510`	If user config `Context Filter` contains `Latitude`
`.longitude`	Indicator.Attribute	Longitude	`.date`	`-97.8220`	If user config `Context Filter` contains `Longitude`
`.asn`	Indicator.Attribute	ASN	`.date`	`AS13335`	If user config `Context Filter` contains `ASN`
`.tld`	Indicator.Attribute	TLD	`.date`	`com`	If user config `Context Filter` contains `TLD`
`.isp`	Indicator.Attribute	ISP	`.date`	`CLOUDFLARENET, US`	If user config `Context Filter` contains `ISP`
`.http_server`	Indicator.Attribute	HTTP Server	`.date`	N/A	If user config `Context Filter` contains `HTTP Server`
`.os`	Indicator.Attribute	Operating System	`.date`	N/A	If user config `Context Filter` contains `Operating System`
`.domain_registered_n_days_ago`	Indicator.Attribute	Domain Registered Days Ago	`.date`	`5`	Updated if already exists. If user config `Context Filter` contains `Domain Registered Days Ago`

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	1 minute
Indicators	46
Indicator Attributes	221

Known Issues / Limitations

- If the option `Phishing URL` is not enabled under the **Indicator Filter** configuration parameter, all the indicators ingested will not be related.

Change Log

- **Version 1.0.0**
  - Initial release