ThreatQuotient

A Securonix Company

WMC Global CDF

Version 1.0.0

August 04, 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

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: 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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The WMC Global CDF integration imports phishing intelligence and compromised credential data from WMC Global into ThreatQ. The integration enables organizations to ingest newly identified phishing URLs, monitor for compromised payment cards and account credentials, and correlate this intelligence with existing ThreatQ data to support phishing investigations, fraud detection, and threat response activities.

Powered by WMC Global's **PhishFeed** and **VicSearch** services, the integration provides visibility into active phishing campaigns and exposed credentials associated with your organization. By centralizing this intelligence within ThreatQ, security teams can more effectively identify targeted attacks, investigate compromised assets, and prioritize response efforts.

The integration provides the following feeds:

- **WMC Global PhishFeed** - ingests new phishing URLs and relevant context from WMC Global's PhishFeed.
- **WMC Global VicSearch** - ingests phishing URLs and compromised credential context from WMC Global's VicSearch.

The integration ingests the following ThreatQ objects:

- Compromised Accounts (custom object)
- Compromised Cards (custom object)
- Indicators (URLs)

Prerequisites

The integration requires the following to install and run the integration:

- A valid **WMC Global API key**. Each feed requires a corresponding WMC Global service license (for example, **PhishFeed** or **CCR/VicSearch**). Contact WMC Global to obtain the licenses required for the feeds you plan to use.
- The Compromised Account and Compromised Card custom objects installed on your ThreatQ instance.

Compromised Account and Card Custom Objects

The integration requires that the Compromised Account and Compromised Card custom objects be installed on your ThreatQ instance.

Use the steps provided to install the custom objects.

> ⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Set your install pathway environment variable. This command will retrieve the install pathway from your configuration file and set it as variable for use during this installation process.

   ```
   INSTALL_CONF="/etc/threatq/platform/install.conf"

   if [ -f "$INSTALL_CONF" ]; then source "$INSTALL_CONF"

   fi
   ```

```
MISC_DIR="${INSTALL_BASE_PATH:-/var/lib/threatq}/misc"
```

5. Navigate to the tmp folder using the environment variable:

```
cd $MISC_DIR
```

6. Upload the custom object files, including the images folder.

   The directory structure should resemble the following:

   - install.sh
   - <custom_object_name>.json
   - images (directory)
     - <custom_object_name>.svg

7. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq --
sh /var/lib/threatq/misc/install.sh /var/lib/threatq/misc
```

   The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

8. Delete the install.sh, definition json file, and images directory from step 6 after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the tmp folder:

```
cd /tmp/
```

5. Create a new directory for the custom object files:

```
mkdir <integration_name>
```

6. Upload the custom object files, including the images folder, to the new directory.
7. Navigate to the integration name directory if you have not done so already.

   The directory structure should be as the following:

   - tmp
     - <integration_name>
       - install.sh
       - <custom_object_name>.json
       - images (directory)
         - <custom_object_name>.svg
8. Run the following command to ensure you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

9. Run the install script:

```
sudo ./install.sh
```

   ⚠ You must be in the directory that houses the install.sh and json file when running this command.

   The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

10. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf <integration_name>
```

Installation

The integration requires that the Compromised Account and Compromised Card custom objects be installed on your ThreatQ instance prior to installing the CDF. Failure to install the custom objects will result in the CDF installation process failing.

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 zip file.
3. Extract and install the required custom objects if you have not done so already.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine
7. Select the individual feeds to install, when prompted and click **Install**.

   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.

The feed(s) 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:

WMC Global PhishFeed Parameters

PARAMETER	DESCRIPTION
API Key	Enter your WMC Global PhishFeed API key. The API key must have permission to access the **PhishFeed** service.
Context Filter	Select the contextual information to import into ThreatQ for each phishing URL. Only the selected fields are ingested. Options include: ◦ Related IP Address *(default)* ◦ Threat Actor Emails *(default)* ◦ Impersonated Brand *(default)* ◦ Phishing Kit Names *(default)* ◦ Is Mobile *(default)* ◦ Country Code *(default)* ◦ Region (State) ◦ City

PARAMETER	DESCRIPTION
	◦ ASN ◦ ASN Organization

WMC Global VicSearch Parameters

PARAMETER	DESCRIPTION
API Key	Enter your WMC Global API key. The API key must have permission to access the **CCR** service.
Brand Filter	Enter a brand name or brand search string to monitor for compromised credentials and phishing URLs. You can use the wildcard character (**`*`**) to search across all brands.
Content Filter	Select the content filter used when searching for compromised credentials and phishing URLs. Options include: ◦ Emails *(default)* ◦ Any Content ◦ Custom Search
Custom Search	Enter a custom search string to use when the **Content Filter** is set to **Custom Search**.
Ingest Potentially Compromised Emails	Enable this parameter to ingest email addresses identified within the matched content of phishing pages. This parameter is useful for identifying potentially compromised user credentials. This parameter is disabled by default.
Ingest Potentially	Enable this parameter to ingest payment card numbers identified within the matched content of phishing pages. Only values that pass **Luhn's Algorithm** are imported. This parameter is useful for identifying potentially

PARAMETER	DESCRIPTION
Compromised Credit Cards	compromised payment cards. This parameter is disabled by default.
Ignore Compromised Cards for Keywords	Enter one keyword per line to exclude false-positive payment card matches. This option helps prevent values such as shipping tracking numbers or other numeric identifiers from being imported as compromised payment cards.

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

WMC Global PhishFeed

The WMC Global PhishFeed feed ingests new phishing URLs and relevant context from WMC Global's PhishFeed.

```
GET https://api.phishfeed.com/v2/feed
```

Sample Response:


```
{
    "count": 10000,
    "data": [
        {
            "id": 38473852,
            "url": "https://address-confirmation-id7451.line.pm/us/
en/homepage%23id10663",
            "ip": "",
            "ip_location": ", , ",
            "ip_as": "",
            "ip_asn": "",
            "date_found": "2024-03-12 13:53:40",
            "brand": "UPS",
            "zip_kits": null,
            "zip_emails": null,
            "mobile": true
        },
        {
            "id": 38473851,
            "url": "https://ups-tracking-id10663.package101.delivery/
redelivery%23id10663",
            "ip": "",
            "ip_location": ", , ",
            "ip_as": "",
            "ip_asn": "",
            "date_found": "2024-03-12 13:53:20",
            "brand": "UPS",
            "zip_kits": null,
            "zip_emails": null,
            "mobile": true
        }
```

```
    ]
}
```

ThreatQuotient provides the following default mapping for this feed *based on each item* within the API response's `data` array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.url	Indicator.Value	URL	.date_found	N/A	N/A
.ip	Indicator.Value	IP Address	.date_found	N/A	Optional
.zip_emails	Indicator.Value	Email Address	.date_found	N/A	Optional
.brand	Indicator.Attribute	Impersonated Brand	.date_found	Facebook	Optional; When value != Undetermined
.zip_kits	Indicator.Attribute	Phishing Kit Name	.date_found	N/A	Optional
.mobile	Indicator.Attribute	Is Mobile	.date_found	true	Optional
.country_code	Indicator.Attribute	Country Code	.date_found	DE	Optional
.region	Indicator.Attribute	Region	.date_found	Virginia	Optional
.city	Indicator.Attribute	City	.date_found	New York	Optional
.ip_as	Related Indicator.Attribute	ASN	.date_found	N/A	Optional
.ip_asn	Related Indicator.Attribute	ASN Organization	.date_found	N/A	Optional
N/A	Indicator.Tag	phishing	.date_found	N/A	Applied to ingested Indicators

WMC Global VicSearch

The WMC Global VicSearch feed ingests phishing URLs and compromised credential context from WMC Global's VicSearch.

`POST https://api.phishfeed.com/vicsearch/v3/search`

Sample Response:

```
{
    "total_records": 3,
    "scroll_id": null,
    "phish_data": [
        {
            "brand": "Facebook",
            "date_time": "2021-01-25T21:02:24",
            "last_version_found": null,
            "version_date_time": "2021-01-25T21:08:15+00:00",
```

```
            "file_name": "http__mobilefbook-
nl6frxck1.nikmehrchap.com_broken.txt",
            "phish_id": 12906858,
            "phish_url": "http://mobilefbook-
nl6frxck1.nikmehrchap.com/",
            "highlight": {
                "total_content_matched": 18,
                "returned_content": 18,
                "matched_content": [
                    "owenkay@bell.net",
                    "jasonwleslie@aol.com",
                    "hashimstubbs@aol.com",
                    "mayhayes91@gmail.com",
                    "rickywrightjr@aol.com",
                    "fishingfool004@gmail.com",
                    "brady_vanessa@yahoo.com",
                    "bkspee@aol.com",
                    "bkspee@aol.com",
                    "bkspee@aol.com",
                    "vhammond88@gmail.com",
                    "vhammond88@gmail.com",
                    "cactusowl@gmail.com",
                    "j.braudis@insightbb.com",
                    "j.braudis@insightbb.com",
                    "j.braudis@insightbb.com",
                    "harabisdebra@yahoo.com",
                    "harabisdebra@yahoo.com"
                ]
            }
        },
        {
            "brand": "Facebook",
            "date_time": "2021-01-22T15:46:39",
            "last_version_found": null,
            "version_date_time": "2021-01-22T15:52:57+00:00",
            "file_name":
"http__comfacebook-47852227.collectifautisme.ma_broken.txt",
            "phish_id": 12859426,
            "phish_url": "http://
comfacebook-47852227.collectifautisme.ma/",
            "highlight": {
                "total_content_matched": 1,
```

```
                "returned_content": 1,
                "matched_content": [
                    "lu1s.v@hotmail.com"
                ]
            }
        },
        {
            "brand": "Undetermined",
            "date_time": "2023-06-01T02:26:41+00:00",
            "file_name": "http__rakuntuls.dynnamn.ru_rzltcc.txt",
            "highlight": {
                "matched_content": [
                    "4430576401452017"
                ],
                "returned_content": 1,
                "total_content_matched": 1
            },
            "last_version_found": true,
            "phish_id": "36848918",
            "phish_url": "http://rakuntuls.dynnamn.ru/",
            "version_date_time": "2023-06-03 04:35:51+00:00"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item within the API response's array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.phish_url	Indicator.Value	URL	.version_date_time	N/A	N/A
.highlight.matched_content[]	Card.Value	N/A	.version_date_time	4430576401452017	Optional; Passes Luhn's Algorithm
.highlight.matched_content[]	Account.Value	N/A	.version_date_time	harabisdebra[@]yahoo.com	Optional; Contains @ character
N/A	Indicator.Tag	phishing	.version_date_time	N/A	Applied to phishing URL
N/A	Account.Tag / Card.Tag	phished	.version_date_time	N/A	Applied to compromised accounts/cards
.brand	Account.Attribute / Card.Attribute	Affected Brand	.version_date_time	N/A	Applied to compromised accounts/cards
.brand	Indicator.Attribute	Impersonated Brand	.version_date_time	N/A	Applied to phishing URL

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.

WMC Global PhishFeed

METRIC	RESULT
Run Time	4 minutes
Indicators	2,549
Indicator Attributes	8,793

WMC Global VicSearch

METRIC	RESULT
Run Time	1 minute
Compromised Accounts	18
Compromised Account Attributes	10
Indicators	3
Indicator Attributes	5

Known Issues / Limitations

- **Complex Content Search Queries -** Highly complex **Custom Search** filters may cause the WMC Global API to time out before results are returned. If you experience timeouts, simplify the search query or contact WMC Global for guidance on optimizing your search criteria.

Change Log

- **Version 1.0.0**
  - Initial release