

ThreatQuotient



VXVault URL CDF Guide

Version 1.0.0

February 08, 2022

ThreatQuotient

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

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

- Support 4
- Versioning..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- ThreatQ Mapping 9
 - VXVault URL 9
- Average Feed Run..... 10
- Change Log..... 11

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 © 2022 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.

Versioning

- Current integration version: 1.0.0
- Compatible with ThreatQ versions \geq 4.3.0

Introduction

The VXVault URL CDF for ThreatQ retrieves a list of malicious URLs.

The integration provides the following endpoint:

- **VXVault URL** - retrieves a list of URLs and ingests them as indicators into the ThreatQ platform.

The integration ingests indicators and indicator attributes into the ThreatQ platform.

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 to open its details page.
4. Review the feed 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

VXVault URL

The VXVault URL feed retrieves a list of URLs and ingests them as indicators into ThreatQ.

```
GET http://vxvault.net/URL_List.php
```

Sample Response:

```
http://91.243.44.99/rev-Hehtcbz.png
http://20.51.217.113/hub/Ngsvpxd.log
http://20.51.217.113/fc/Xxzjxsyby.exe
http://20.51.217.113/ome/Xxzjxsyby.jpg
http://integralbd.com/inquiry-cim.jpg
http://94.250.249.239/Software/02015/FreeMatPortable_4_3_English.jpg
https://scottbyscott.com/obino/obs.png
https://store1.gofile.io/download/9c3dfe5f-3155-44f2-98f2-24ce360b1f7a/winit.exe
http://integralbd.com/Ematlm.jpg
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
1 (first token)	Indicator.Value	URL	http://91.243.44.99/rev-Hehtcbz.png	N/A

Average Feed Run

METRIC	RESULT
Run Time	3 minutes
Indicators	100
Indicators Attributes	100



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.

Change Log

- Version 1.0.0
 - Initial release