ThreatQuotient

DomainTools Hotlist CDF

Version 1.0.0

November 19, 2024

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	>= 5.24.1
Support Tier	ThreatQ Supported

Introduction

The DomainTools Hotlist CDF surfaces a list of active high-risk domains.

The Domain Hotlist is a family of hotlists that support blocking with DNS Response Policy Zones (RPZ). The hotlist configurations support smaller DNS servers/firewalls with fixed or limited resources, as well as large DNS fleets. Activity is measured by DomainTools' global passive DNS sensor network and domain risk is calculated from predicted malware and phishing activity, and observed proximity with malicious infrastructure. Hotlists are available from DomainTools' DNS servers using DNS Zone Transfer from an authorized IP address.

> Each hotlist is updated once per day. Some hotlists are capped at a maximum number of entries.

The integration provides the following feed:

- **DomainTools Hostlist 95 RPZ -** ingests FQDN indicators from DomainTools.

The integration ingests FQDN type indicators into the ThreatQ platform.

Prerequisites

The following is required to utilize the integration:

- DomainTools Username and API Key.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. 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
6. 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.

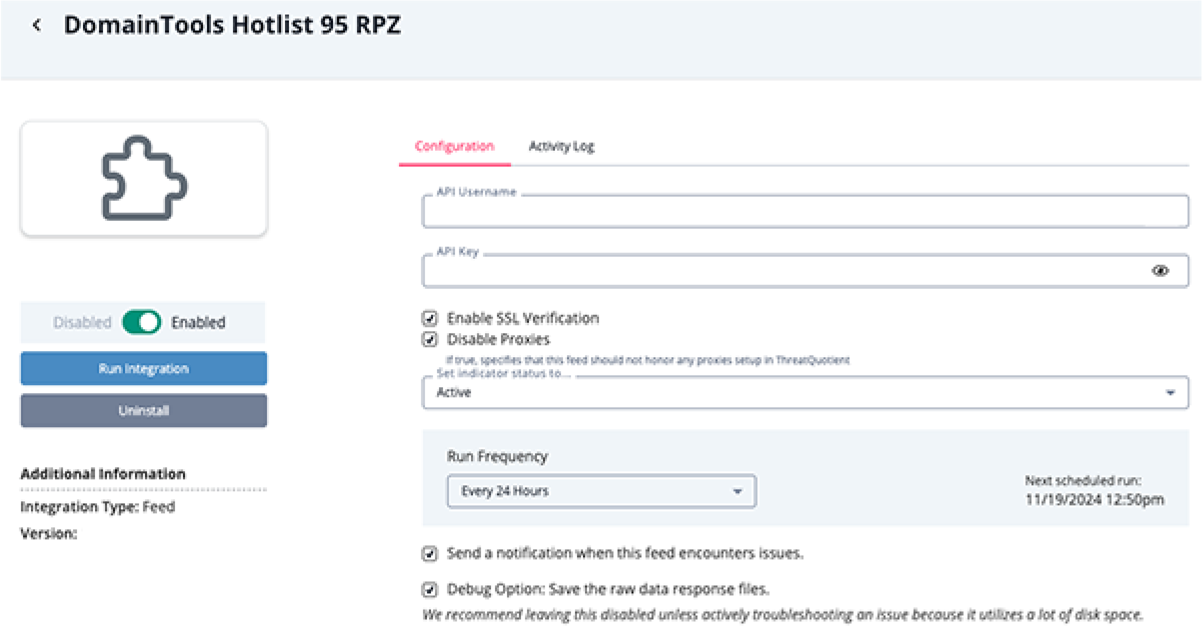
To configure the integration:

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:

PARAMETER	DESCRIPTION
API Username	Enter your DomainTools Hostlist username.
API Key	Enter your DomainTools Hostlist API Key.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.



‹ DomainTools Hotlist 95 RPZ

API Username

API Key

☑ Enable SSL Verification

☑ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Set indicator status to...: Active

Run Frequency: Every 24 Hours

Next scheduled run: 11/19/2024 12:50pm

☑ Send a notification when this feed encounters issues.

☑ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Disabled / Enabled

Additional Information

Integration Type: Feed

Version:

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

DomainTools Hotlist 95 RPZ

The DomainTools Hostlist 95 RPZ feed ingests a list of active, high risk domains which has activity being measured by DomainTools' global passive DNS sensor network.

`GET https://api.domaintools.com/v1/download?api_username={username}&api_key={api_key}6&scope=domain_hotlist_tmo`

Sample Response:

```
{
    "response": {
        "download_name": "domain_hotlist_tmo",
        "files": [
            {
                "name": "domain_hotlist_tmo/tmo.domainhotlist.gz",
                "last_modified": "2024-11-05T01:03:04+00:00",
                "etag": "\"371978a570051763df5214a06717a34e\"",
                "size": "2016065",
                "url": "https://d2mzrdiuqyylox.cloudfront.net/
domain_hotlist_tmo/tmo.domainhotlist.gz?
&Expires=1731462131Signature=bKoiKd8Rcc1pv1ghMzmE3~7tB9f5YQ98Jec9ep-
~QkwiBjjD0RA5sf2-Xb6tD0S8gYU4FLORXhyUggFFFKxf4nUtkYSnJJzbYlUweUfgut0fBnlgsK1-
sU4eXrG8wxOfdAWyBgNQ6ovA7yHzfX0aXpPIeelJtHY33XjpHQzJBz6s0BmP1ErSuQmuW3zrf2lRxyW
yLb3f8eLVBtLstMOKa2UvBi1t9FR~hiQGR4DEnBrvy5WQ4alvwF6hc~sU9rKxqnIIRfjeHqHpTS3Qa3
Ki~vxw64XkfUW5YM-Cb0~fBO0pmajmUXRkrv2q1BIDQxLKAy0fWhMEtrSp~VEGdJTbFg__&Key-
Pair-Id=KJPH4C4RWZJ32"
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`value[]`	Indicator.value	FQDN	N/A	`1wzbpb.top`	Value received from downloading the response.url
['DomainTools', 'Hotlist 95 RPZ']	Indicator.tag	N/A	N/A	`DomainTools`	All indicators have 'DomainTools' and 'Hotlist 95 RPZ' tags

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	16 minutes
Indicators	347,358

Change Log

- **Version 1.0.0**
  - Initial release