ThreatQuotient

CIRCL Passive DNS Operation Guide

Version 1.0.0

February 14, 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

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.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.57.2`

Introduction

The CIRCL Passive DNS operation for ThreatQ allows users to query the CIRCL Passive DNS database for selected indicators in the ThreatQ Threat Library.

The operation provides the following action:

- **Query CIRCL Passive DNS** - queries the Query CIRCL Passive DNS database for FQDN and IP Address indicator sub-types.

> See the Actions chapter for more information on the action listed above.

The operation is compatible with the following indicator types:

- FQDN
- IP Address

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 operation 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 operation and will require user confirmation before proceeding.

6. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* 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. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname/IP Address of the CIRCL server	The hostname or IP address of the Circl instance. The system default is for the cloud offering: global.cloud.Circl.com.
Communication Port	Optional - Enter the user port used for communication with CIRCL.
User Token	Your User Token for authentication.
Use HTTP	Enable this option to use HTTP protocol when connecting to CIRCL.
Verify SSL	Enable this option to verify the SSL when connecting to CIRCL.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The CIRCL Passive DNS operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query CIRCL Passive DNS	Query Passive DNS database for the selected indicators.	Indicators	FQDN, IP Address

Query CIRCL Passive DNS

The Query CIRCL Passive DNS action queries the database for for FQDN and IP Address indicator sub-types.

```
GET https://<Circl Host>/pdns/query/<indicators>
```

Sample Response:

```
{
  "count": 6,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1496995637,
  "rrtype": "A",
  "rrname": "www.threatq.com",
  "rdata": "104.196.175.197",
  "time_last": 1499951111
}{
  "count": 3,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1495523983,
  "rrtype": "NS",
  "rrname": "threatsketch.com",
  "rdata": "dns04.gpn.register.com",
  "time_last": 1495533768
}{
  "count": 3,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1495523983,
  "rrtype": "NS",
  "rrname": "threatsketch.com",
  "rdata": "dns01.gpn.register.com",
  "time_last": 1495533768
}{
  "count": 3,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1495523983,
  "rrtype": "NS",
  "rrname": "threatsketch.com",
  "rdata": "dns02.gpn.register.com",
  "time_last": 1495533768
}{
  "count": 3,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1495523983,
  "rrtype": "NS",
  "rrname": "threatsketch.com",
  "rdata": "dns05.gpn.register.com",
  "time_last": 1495533768
}{
  "count": 3,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1495523983,
  "rrtype": "NS",
  "rrname": "threatsketch.com",
  "rdata": "dns03.gpn.register.com",
  "time_last": 1495533768
}{
  "count": 5,
  "origin": "https://www.circl.lu/pdns/",
  "time_first": 1495523983,
  "rrtype": "A",
  "rrname": "threatsketch.com",
  "rdata": "104.196.175.197",
  "time_last": 1495533768
}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.rrtype	Indicator	indicator.name.Resource Type	NA	A
response.rrdata	Indicator	attribute.name.Resource Data	NA	123.321.156.90

Change Log

- **Version 1.0.0**
    - Initial Release