ThreatQuotient

DCSO TIE CDF Guide

Version 1.0.1

July 27, 2022

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

Integration Details 5
Introduction 6
Prerequisites 7
DCSP TIE Access Token 7
Installation 8
Configuration 9
ThreatQ Mapping 12
DCSO TIE 12
IoC Type Mapping 14
Average Feed Run 15
Known Issues / Limitations 16
Change Log 17

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	1.0.1
Compatible with ThreatQ Versions	>= 4.49.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/dcso-tie-cdf

Introduction

The DCSO TIE feed ingests IoCs and related attributes from DCSO's TIE using the following endpoint:

- **DCSO TIE** - ingests indicators with related attributes.

The integration ingests the following indicator sub-types:

- FQDN
- URL
- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- Fuzzy Hash
- Filename
- Email Address
- ASN
- CIDR Block

The indicators ingested will have the following attributes:

- Minimum and Maximum Severity
- Minimum and Maximum Confidence
- Actors
- Families
- Categories
- Entities

Prerequisites

Review the follow prerequisite before attempting to install the CDF.

DCSP TIE Access Token

You will need your DSCO TIE Access Token in order to use the DSCO TIE CDF integration. You can find your DCSO TIE access token on your DCSO TIE instance under **Settings > Access Tokens**.

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:

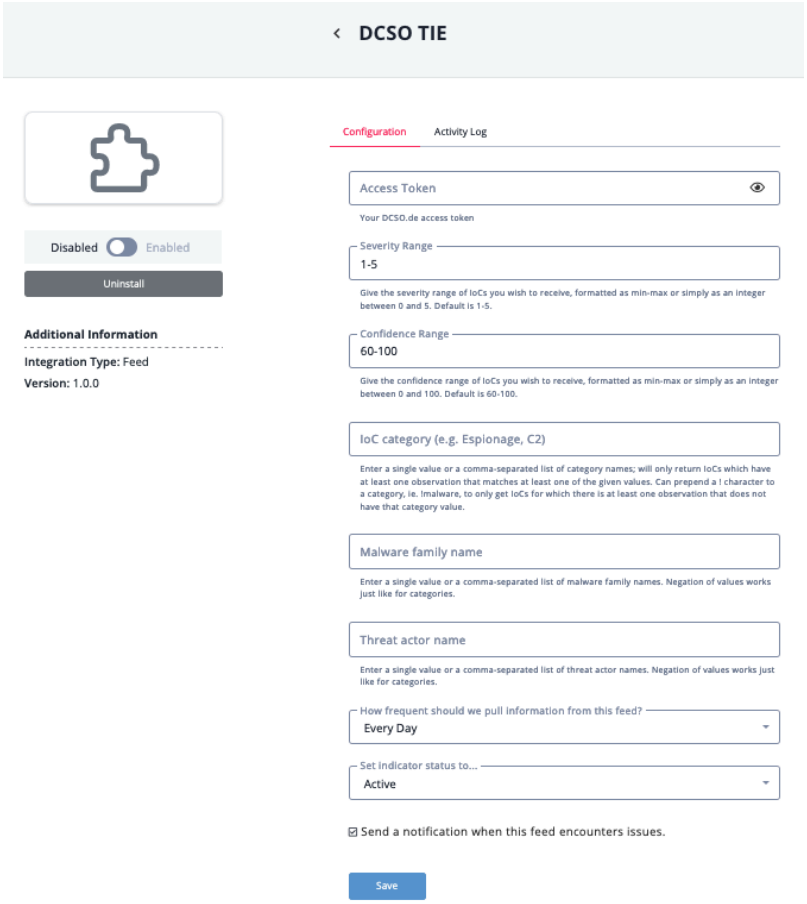
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
Access Token	Your DCSO.de access token to use for authentication.
Severity Range	The severity range of IoCs you wish to receive, formatted as min-max or simply an integer between 0 and 5. The default setting is 1-5.
Confidence Range	The confidence range of IoCs you wish to receive, formatted as min-max or simply an integer between 0 and 100. The default setting is 60-100.
IOC Category	Enter a single value or a comma-separated list of category names. If given, the integration will only return data which have at least one observation that matches at least one of the given values, or (if match_all includes category) all of the given values. You can prepend a **!** character to a category to get only IoCs that do not have that IOC category name. **Example:** !malware.

PARAMETER	DESCRIPTION
Malware Family Name	Enter a single value or a comma-separated list of malware family names (as returned by the families endpoint). If given, the integration will only return data which have at least one observation that matches at least one of the given values, or (if match_all includes family) all of the given values. This entry can be negated by prepending a ! character. **Example:** `! tesla` will only show data for which there is at least one observation that is not related to a tesla malware.
Threat Actor Name	Enter a single value or a comma-separated list of threat actor names (as returned by the threat actor endpoint). If given, the integration will only return data which have at least one observation that matches at least one of the given values, or (if match_all includes threat actor) all of the given values. This entry can be negated by prepending a ! character. **Example:** `! fin7` will only show data for which there is at least one observation that is not related to a fin7 threat actor.



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

DCSO TIE

The DCSO TIE feed ingests ThreatQ indicators and related attributes.

`GET https://tie.dcso.de/api/v1/iocs`

Sample Response:


```
{
  "has_more": true,
  "params": {
    "direction": "desc",
    "limit": 10,
    "confidence": "60-100",
    "severity": "1-5",
    "offset": 0,
    "order_by": "created_at"
  },
  "iocs": [
    {
      "data_type": "DomainName",
      "actors": [
        "bengal"
      ],
      "categories": [
        "c2-server"
      ],
      "families": [
        "andromeda"
      ],
      "first_seen": "2016-09-28 17:07:24.216720+02:00",
      "last_seen": "2016-09-28 17:07:24.216720+02:00",
      "created_at": "2016-09-28 18:03:47.138723+02:00",
      "updated_at": "2016-09-28 18:03:47.138723+02:00",
      "id": "3c5db453-873f-4107-994b-d27389de94e1",
      "max_confidence": 100,
      "max_severity": 3,
      "min_confidence": 80,
      "min_severity": 2,
      "entity_ids" : [
        "D7F7D360-DABE-30DF-B1ED-D72892ADA72D"
      ],
      "n_occurrences": 2,
      "sources": [
        "malwaredomainlist",
        "payload_security"
      ],
      "value": "www.ozowarac.com"
    },
    #...
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
iocs[].value	Indicator	.iocs[].data_type	N/A	www.ozowarac.com	See the IoC Type mapping below to see how the indicator type is converted from DCSO TIE to TQ.
.iocs[].min_severity	Attribute	Minimum Severity	N/A	2	N/A
.iocs[].max_severity	Attribute	Maximum Severity	N/A	3	N/A
.iocs[].min_confidence	Attribute	Minimum Confidence	N/A	80	N/A
.iocs[].max_confidence	Attribute	Maximum Confidence	N/A	100	N/A
.iocs[].actors	Attribute	Actor	N/A	bengal	N/A
.iocs[].families	Attribute	Family	N/A	andromeda	N/A
.iocs[].categories	Attribute	Category	N/A	c2-server	N/A
.iocs[].entity_ids	Attribute	Entity ID	N/A	D7F7D360-DABE-30DF-B1ED-D72892ADA72D	N/A

IoC Type Mapping

ThreatQuotient provides the following IoC type mapping:

DCSO TIE DATA TYPE VALUE	THREATQ INDICATOR TYPE VALUE
DomainName	FQDN
URLVerbatim	URL
ExactHash (where `value` starts with `md5`)	MD5
ExactHash (`value` starts with `sha1`)	SHA-1
ExactHash (`value` starts with `sha256`	SHA-256
ExactHash (`value` starts with `sha384`	SHA-384
ExactHash (`value` starts with `sha512`	SHA-512
SSDEEP	Fuzzy Hash
IPv4	CIDR Block and IP Address (without netmask)
IPv6	IPv6 Address
FileName	Filename
Email	Email Address
Layer4Endpoint	IP Address
ASN	ASN

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.

The following run is working with 1 hour worth of data from DCSO TIE - from February 9, 2022 at 4:09pm to February 9, 2022 at 5:09pm.

METRIC	RESULT
Run Time	11 minutes
Indicators	3,959
Indicator Attributes	21,218

Known Issues / Limitations

- DCSO's TIE can encompass a large amount of IoCs. When this number is especially high (~ >20000), the feed will throw a 504 Gateway Time-out error. This error is caused by DCSO TIE servers.

  To avoid this error, this feed has several configuration options (Severity, Confidence, Query Time Range) to limit the number of IoCs being ingested to a more reasonable amount. ThreatQuotient strongly recommends that users utilize these configurations to keep the feed query time range configuration between 1-2 hours.

  The same 504 Gateway Time-out error can also be caused if incompatible configurations are entered. This will cause the server to continuously load to find IoCs with the specified parameters but finding none and timing out. This error will not stop the feed run.

Change Log

- **Version 1.0.1**
  - IP Addresses are now ingested as CIDR Blocks and IP Addresses (without netmask) in ThreatQ. See the IoC Type Mapping section for more details.
- **Version 1.0.0**
  - Initial release