ThreatQuotient

DCSO TIE Operation Guide

Version 1.0.0

February 23, 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.

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 >= `4.57.2`

Introduction

The DCSO TIE Operation enriches indicators of compromise from the DCSO Threat Intelligence Database.

The operation provides the following action:

- **Search DCSO** - Queries the DCSO TIE database for indicators of compromise.

See the Actions chapter for more information on this action.

The integration is compatible with the following indicator types:

- ASN
- MD5
- Email Address
- Filename
- FQDN
- Ip Address
- SHA-1

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	Enter the hostname or IP address of DCSO TIE. The default entry is `tie.dcso.de`.
Access Token	Enter the access token for authenticating with the DCSO TIE.
Use HTTP Proxy	This option allows you to use the HTTP proxy configured on the ThreatQ platform. This information can be access on the Proxy tab under System Configurations (Site Settings > System Configurations).
Verify SSL	This option allows you to verify the SSL when connecting to the DCSO TIE.

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

Actions

The DCSO TIE operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Search DCSO TIE	Query DCSO TIE database for indicators of compromise.	Indicators	IP Address, FQDN, URL, Email Address, MD5, SHA-1, SHA-256, Filename, ASN

Search DCSO TIE

The Search DCSO TIE action queries DCSO TIE database for indicators of compromise.

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

Sample Response:


```
{
    "iocs": [
        {
            "enrichment_requested_at": null,
            "enrich": false,
            "observations": [
                {
                    "actors": [],
                    "severity": 1,
                    "created_at": "2020-05-26 03:03:26.304262+00:00",
                    "seq": 11039188892,
                    "entities": [],
                    "confidence": 90,
                    "id": "f91445a8-8874-4c5d-b6f3-c605cf281a2a",
                    "first_seen": "2020-05-26 02:37:55+00:00",
                    "categories": [
                        "c2-server"
                    ],
                    "attributes": [
                        {
                            "name": "killchain",
                            "value": "c2"
                        },
                        {
                            "name": "maliciousconfidence",
                            "value": "high"
                        },
                        {
                            "name": "threattype",
                            "value": "criminal"
                        },
                        {
                            "name": "threattype",
                            "value": "downloader"
                        },
                        {
                            "name": "malware",
                            "value": "guloader"
                        }
                    ],
                    "families": [
                        "guloader"
                    ],
                    "updated_at": "2021-12-09 20:38:56.732630+00:00",
                    "event": {
                        "source": {
                            "pseudonym": "322a92d8"
                        },
```

```
                    "attributes": [],
                    "id": "f567bb45-7de8-4678-9d41-31afaa6781c9"
                },
                "last_seen": "2021-12-09 18:35:59+00:00"
            }
        ],
        "created_at": "2020-05-26 03:03:11.013208+00:00",
        "value": "www.microsoft.com.software-download.trillium.cam",
        "hotness": 0.0,
        "id": "18b2acfe-4e00-4168-a042-0a1616125451",
        "t_1": null,
        "data_type": "DomainName",
        "gamma": 3.85e-06,
        "a_1": null,
        "comment": null,
        "attributes": [],
        "updated_at": "2020-05-26 03:46:06.311661+00:00",
        "enriched_at": "2020-05-26 03:46:06.320990+00:00"
    },
    {
        "enrichment_requested_at": null,
        "enrich": false,
        "observations": [
            {
                "actors": [],
                "severity": 2,
                "created_at": "2020-03-16 14:40:18.252615+00:00",
                "seq": 7227070859,
                "entities": [],
                "confidence": 80,
                "id": "ab80c10c-384f-4bbd-aee3-3c3e00965ef8",
                "first_seen": "2020-03-16 14:56:56+00:00",
                "categories": [],
                "attributes": [],
                "families": [],
                "updated_at": "2020-03-16 16:10:20.096090+00:00",
                "event": {
                    "source": {
                        "pseudonym": "a9f4058d"
                    },
                    "attributes": [
                        {
                            "name": "info",
                            "value": "Suspicious code signing certificate:
467cd9d2432a26496bea2ae6d90c36cfe34c99d9"
                        },
                        {
                            "name": "misp-uuid",
                            "value": "5e6f7a14-2fc0-4248-8d09-0250ac12042b"
                        }
                    ],
                    "id": "57bc4f80-2b4f-4bcd-a06b-aaf3bfca8932"
                },
                "last_seen": "2020-03-16 14:56:56+00:00"
            }
        ],
        "created_at": "2020-03-16 14:40:18.017528+00:00",
        "value": "www.microsoft.com.msonlinemicrosoft.com",
        "hotness": 0.0,
        "id": "14ce5bc0-d97d-4f9c-8bd4-3f47a5824959",
        "t_1": null,
```

```
            "data_type": "DomainName",
            "gamma": 3.85e-06,
            "a_1": null,
            "comment": null,
            "attributes": [],
            "updated_at": "2020-03-16 15:07:25.382572+00:00",
            "enriched_at": "2020-03-16 15:07:25.391472+00:00"
        }
    ],
    "has_more": false,
    "params": {
        "enriched": false,
        "severity": "1-",
        "date_format": "default",
        "category": "!parking,!sinkhole,!deleted,!potential-false-positive",
        "direction": "desc",
        "value": "www.microsoft.com",
        "filter": "default",
        "last_seen_since": "2020-01-29T17:13:42Z",
        "confidence": "60-",
        "data_type": "DomainName",
        "order_by": "last_seen",
        "no_defaults": false,
        "match_all": "",
        "offset": 0,
        "exact": false,
        "limit": 50
    }
}
```


ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.iocs[].value	Value	Indicator (.iocs[].data_type)	.data[].first_seen	www.microsoft.com.msonlinemicrosoft.com
.iocs[].hotness	Attribute	Hotness	.data[].first_seen	0.0
.iocs[].gamma	Attribute	Gamma	.data[].first_seen	3.85e-06
.iocs[].observations[].severity	Attribute	Severity	.data[].first_seen	2
.iocs[].observations[].confidence	Attribute	Confidence	.data[].first_seen	80
.iocs[].observations[].first_seen	Attribute	First Seen	.data[].first_seen	"2020-03-16 14:56:56+00:00"
.iocs[].observations[].last_seen	Attribute	Last Seen	.data[].first_seen	"2020-03-16 14:56:56+00:00"
.iocs[].observations[].categories	Attribute	Categories	.data[].first_seen	["c2-server"]

Configuration Options

The action has the following optional configuration options:

> These options are available upon operation execution.

CONFIGURATION OPTION	DESCRIPTION
Confidence	Enter a value or range for the confidence of the observation.
Severity	Enter a value or range for the severity of the observation.
Wildcard Prefix	Enter a wildcard prefix for searching (e.g. %microsoft.com).
Wildcard Suffix	Enter a wildcard suffix for searching (e.g. microsoft.com%).
Last Seen Since	Enter the date for the last seen sighting (format: YYYY-MM-DD).
Category	Enter a single value or a comma-separated list of category names.
Family	Enter a single value or a comma-separated list of malware family names.
Actor	Enter a single value or a comma-separated list of threat actor names.

Change Log

- **Version 1.0.0**
  - Initial Release