ThreatQuotient

Dragos CDF Guide

Version 1.0.0

February 01, 2021

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

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

Contents

Versioning

- Current Integration Version: `1.0.0`
- Supported on ThreatQ Version: >= `4.34.0`

Introduction

The Dragos CDF retrieves data using the following endpoints:

- `https://portal.dragos.com/api/v1/products`
- `https://portal.dragos.com/api/v1/indicators`

The provider returns Reports and the following Indicator types: MD5, SHA-1, SHA-256, FQDN, and IP Address.

The integration uses basic HTTP authentication based on API Token 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 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 to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Dragos API Key.
API Token	Your Dragos API Token.

Dragos Products

The Dragos Products feed provides the following optional configuration parameter:

PARAMETER	DESCRIPTION
Ingest TLP	If Dragos provides the TLP and this configuration parameter is set to True, the TLP value of the Indicator will be overwritten if it already exists in the ThreatQ system. The default setting is False.

5. Review the **Settings** configuration, 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

Dragos Products

```
GET https://portal.dragos.com/api/v1/products
```


```
{
  "products": [
      {
        "tlp_level": "AMBER",
        "title": "WorldView Special - 04212017 - NYC/SFO Power Outages",
        "executive_summary": "On 21 April 2017 two separate power outages, one in San Francisco and one in New York City raised the concern of a potential cyber-attack from customers and media outlets. There were other localized outages elsewhere in the United States, such as in Boston and Chicago, which some conflated in the same event causing more alarm.",
        "updated_at": "2018-10-15T17:50:28.000Z",
        "threat_level": 0,
        "serial": "WVS-2017-02",
        "ioc_count": 1,
        "tags": [
          {
            "text": "Electric Distribution",
            "tag_type": "Industry"
          },
          {
            "text": "United States",
            "tag_type": "GeographicLocation"
          },
          {
            "text": "Electric Utility",
            "tag_type": "Industry"
          }
        ],
        "release_date": "2017-04-21T04:00:00.000Z",
        "type": "WorldView Special",
        "report_link": "https://portal.dragos.com/api/v1/products/WVS-2017-02/report",
        "ioc_link": "https://portal.dragos.com/api/v1/indicators/WVS-2017-02/report"
      }
  ],
  "total": 240,
  "page": 209,
  "page_size": 50,
  "total_pages": 210
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.products[].title	Report.Value	N/A	.updated_at	WorldView Special - 04212017 - NYC/SFO Power Outages	
.products[].tlp_level	Report.TLP	N/A	N/A	Amber	If Dragos provides the TLP and this configuration parameter is set to True, the TLP value of the Indicator will be overwritten if it already exists in the ThreatQ system
.products[].threat_level	Report.Attribute	Threat Level	.updated_at	2018-10-15 17:50:28.000	
.products[].type	Report.Attribute	Type	.updated_at	WorldView Special	
.products[].report_link	Report.Attribute	Report Link	.updated_at	https://portal.dragos.com/api/v1/products/WVS-2017-02/report	
.products[].ioc_link	Report.Attribute	IOC Link	.updated_at	https://portal.dragos.com/api/v1/indicators/WVS-2017-02/report	
.products[].tags[].text	Report.Attribute	`.tags[].tag_type`	.updated_at	Electric Distribution	

If `..products[].ioc_count` is non-zero, a supplemental call to the `Dragos Indicators` endpoint is made to fetch Indicators related to the Report.

Dragos Indicators

```
GET https://portal.dragos.com/api/v1/indicators
```


```
{
  "indicators": [
     {
        "id": 22673,
        "value": "167.114.213.199",
        "indicator_type": "ip",
        "category": "Network activity",
        "comment": "Indicator associated with SolarWinds supply chain compromise activity and SunBurst malware. ",
        "first_seen": "2020-12-14T17:13:17.000Z",
        "last_seen": "2020-12-14T17:17:00.000Z",
        "updated_at": "2020-12-15T01:50:02.000Z",
        "confidence": "moderate",
        "kill_chain": "Stage1:Exploit",
        "uuid": "4152912c-bace-4557-af74-3f4db66d4d1c",
        "status": "released",
        "activity_groups": [ "ALLANITE" ],
        "attack_techniques": [
          "Command and Control:Application:Layer Protocols:Web Protocols",
          "Initial Access:Supply Chain Compromise"
        ],
        "pre_attack_techniques": [],
        "products": [
            {
              "serial": "AA-2020-38"
            }
        ]
     }
  ],
  "total": 170,
  "page": 70,
  "page_size": 50,
  "total_pages": 71
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].value	Indicator.Value	Mapping using `Indicator Mapping` based on the value of `.indicators[].indicator_type`	.first_seen	167.114.213.199	
.indicators[].category	Indicator.Attribute	Category	.first_seen	Network activity	
.indicators[].status	Indicator.Attribute	Status	.first_seen	release	
.indicators[].confidence	Indicator.Attribute	Confidence	.first_seen	moderate	
.indicators[].kill_chain	Indicator.Attribute	Kill Chain	.first_seen	Stage1:Exploit	
.indicators[].activity_groups[]	Related Adversary			ALLANITE	
.indicators[].attack_techniques[]	Related Attack Pattern			Initial Access:Supply Chain Compromise	Linked to already existing TQ MITRE Attack Pattern

Indicator Mapping

DRAGOS TYPE	TQ INDICATOR TYPE
ip	IP Address
domain	FQDN
md5	MD5
sha1	SHA-1
sha56	SHA-256

Average Feed Run

Feed runtime is 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.

Dragos Products

METRIC	RESULT
Run Time	36 minutes
Indicators	1234
Indicator Attributes	7323
Reports	38
Reports Attributes	300

Dragos Indicators

METRIC	RESULT
Run Time	53 minutes
Indicators	17210
Indicator Attributes	57476
Attack Patterns	38
Adversaries	13

Known Issues / Limitations

- MITRE ATT&CK Attack Patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK Attack Patterns to be related to Indicators. The following feeds ingest MITRE ATT&CK Attack Patterns:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE PRE-ATT&CK
- For the Dragos Products feed, if Dragos provides the TLP and the configuration parameter **Ingest TLP** is set to **True**, the TLP value of the Indicator will be overwritten if it already exists in the ThreatQ system.

Change Log

- **Version 1.0.0**
  - Initial release