ThreatQuotient

A Securonix Company

Dragos OT CDF

Version 1.0.0

November 18, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Dragos OT Cases Configuration Parameters 9
Dragos OT Notifications Configuration Parameters 10
ThreatQ Mapping **14**
Dragos OT Cases 14
Dragos OT Notifications 16
Severity Mapping 21
Average Feed Run **22**
Dragos OT Cases 22
Dragos OT Notifications 23
Change Log **24**

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 © 2025 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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Dragos OT CDF integration for ThreatQ enables organizations to automatically ingest notifications and cases from the Dragos OT (Operational Technology) platform, which provides comprehensive asset visibility and continuous network monitoring for industrial control systems (ICS). Leveraging specialized threat intelligence, advanced detection capabilities, and risk-based playbooks, Dragos OT identifies malicious activity, vulnerabilities, and misconfigurations across OT environments. Integrating this data into ThreatQ allows security teams to correlate OT insights with broader threat intelligence, gaining a unified view of their security posture and strengthening the protection of critical infrastructure.

The integrations provide the following feeds:

- **Dragos OT Cases** - ingests cases as events along with the relevant notifications discovered by Dragos OT.
- **Dragos OT Notifications** - ingests notifications as events along with the affected assets, discovered by Dragos OT.

The integration ingests the following system object types:

- Assets
- Attack Patterns
- Events
- Indicators
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A Dragos OT Deployment.
- A Dragos OT API Key ID.
- A Dragos OT API Secret.
- The user associated with the API Key ID and Secret should have the following permissions:
  - `notification:read`
  - `case:read`

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:

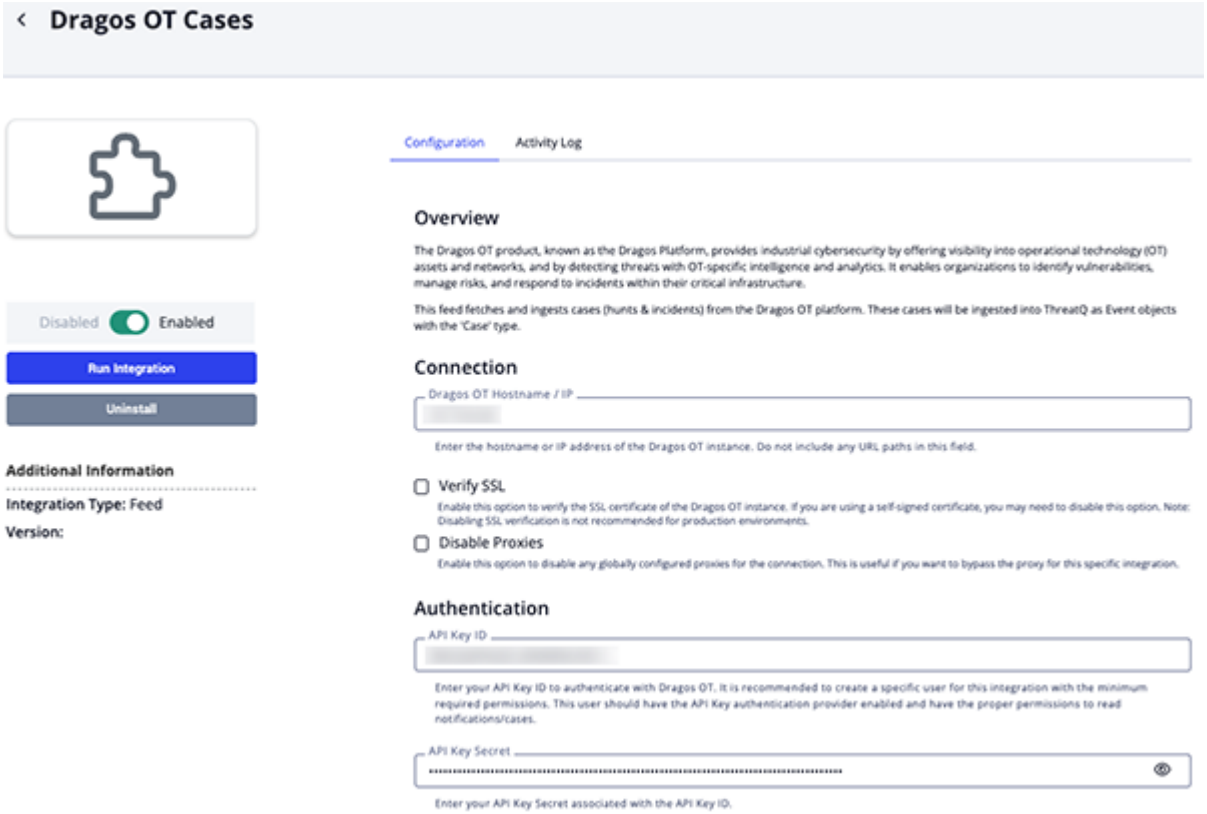
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

Dragos OT Cases Configuration Parameters

PARAMETER	DESCRIPTION
Dragos OT Hostname / IP	Enter the hostname or IP address of the Dragos OT instance. Do not include any URL paths in this field.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
API Key ID	Enter your API Key ID to authenticate with Dragos OT. It is recommended to create a specific user for this integration with the minimum required permissions. This user should have the API Key authentication provider enabled and have the proper permissions to read notifications/cases.
API Key Secret	Enter your API Key Secret associated with the API Key ID.

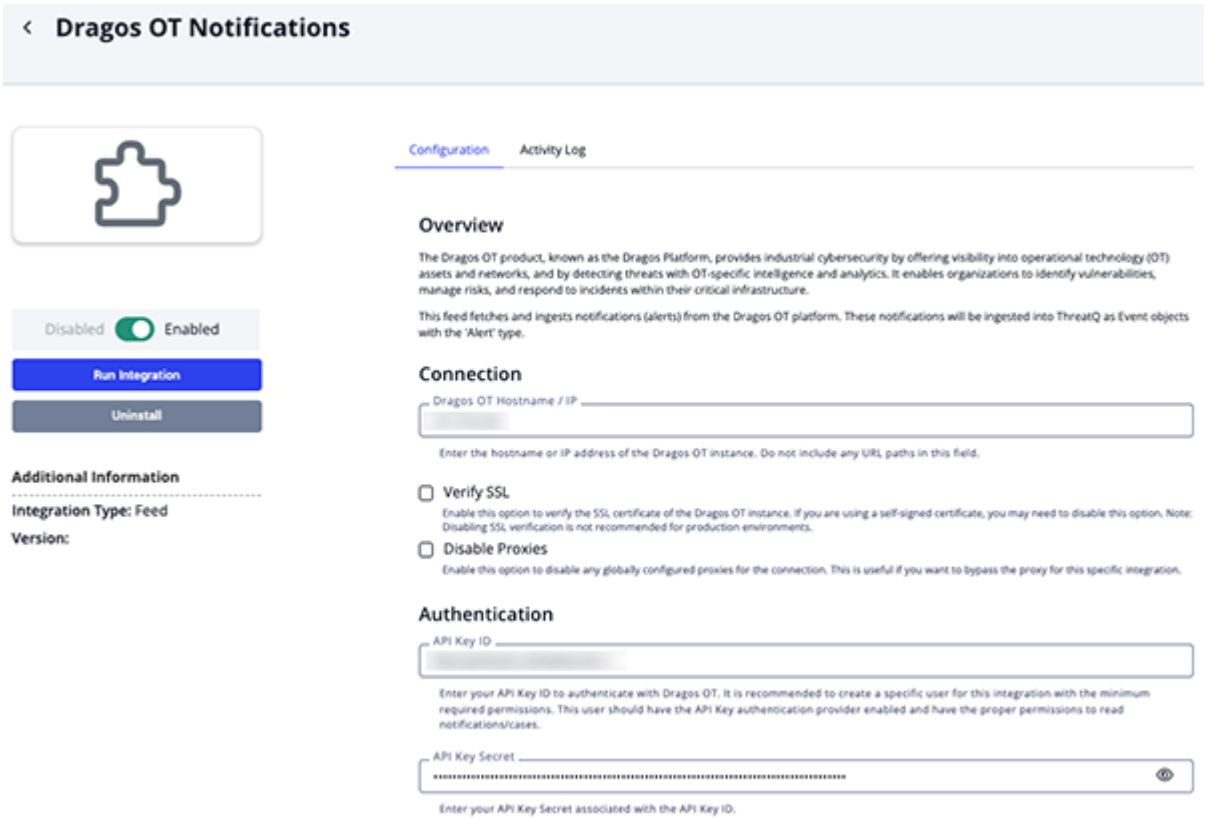


Dragos OT Notifications Configuration Parameters

PARAMETER	DESCRIPTION
Dragos OT Hostname / IP	Enter the hostname or IP address of the Dragos OT instance. Do not include any URL paths in this field.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
API Key ID	Enter your API Key ID to authenticate with Dragos OT. It is recommended to create a specific user for this integration with the minimum required permissions. This user should have the API Key authentication provider enabled and have the proper permissions to read notifications/cases.

PARAMETER	DESCRIPTION
API Key Secret	Enter your API Key Secret associated with the API Key ID.
Minimum Severity	Enter the minimum severity threshold required for the notification to be ingested. The severity is a numeric value ranging from 0 to 5, where `0` is the lowest severity and `5` is the highest. The default value is 3.
Notification State Filter	Select the notification states to ingest in the feed. Options include: ◦ Unresolved *(default)* ◦ Accepted *(default)* ◦ Muted
Additional Filter	Enter any additional FIQL filters, using valid FIQL syntax, to apply to the notifications that will be added to the default filter string. For example, you can filter by notification type. The default value is `(type!='Baseline', (type=='Baseline';parentNotificationId=exists=false))`. See https://fiql-parser.readthedocs.io/en/stable/usage.html for more information on constructing FIQL filters.
Fetch Child Notifications	Enable this parameter to fetch child notifications of the primary notifications including all notifications that are related to the selected notifications. This parameter is disabled by default. Enabling this parameter may increase the number of notifications ingested and will increase the number of API calls made to the Dragos OT instance.
Ingest Affected Assets As	Select how asset information will be ingested into ThreatQ. Options include: ◦ Part of the Object Description *(default)* ◦ As Asset Objects ◦ Do Not Ingest
Apply Asset Tags to Ingested Notifications	Enable this parameter to apply asset tags to the ingested notifications (Event Objects).

PARAMETER	DESCRIPTION
	This will assist in categorizing and filtering the notifications based on asset tags.
Ingest MITRE ATT&CK Tactics as Tags	Enable this to ingest MITRE ATT&CK tactics as tags to the notifications (Event Objects). This parameter is enabled by default.
Notification Context Selection	Select which pieces of context to ingest with each notification (Event Object). Options include: ◦ Severity *(default)* ◦ Severity Score ◦ Source ◦ Count ◦ Detection Type *(default)* ◦ Notification Type *(default)* ◦ Is Reviewed *(default)* ◦ Is Retained *(default)*
Ingest CVEs As	Select the entity type to ingest CVE IDs as in ThreatQ. Options include: ◦ Vulnerabilities ◦ Indicators *(default)*



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

Dragos OT Cases

The Dragons OT Cases feed ingests cases along with the relevant notifications discovered by Dragos OT. Cases will be ingested as Event objects and will be related to the other Event objects that represent the notifications within the case.

`GET https://{{ host }}/cases/cases`

Sample Response:

```
{
    "pageNumber": 1,
    "totalCount": 1,
    "content": [
        {
            "id": 1,
            "name": "CobaltStrike Investigation",
            "hypothesis": "Detection of CobaltStrike activity on the OT
network.",
            "visibility": "PUBLIC",
            "status": "OPEN",
            "priority": 4,
            "incident": false,
            "creator": "admin",
            "createdAt": "2025-05-01T18:21:07Z",
            "updatedAt": "2025-05-05T19:57:39Z",
            "notificationIds": [
                123
            ],
            "watchersCount": 0,
            "justification": "New Journal Entry",
            "assignee": null
        }
    ],
    "pageSize": 50,
    "totalPages": 1
}
```

Notification ids are parsed and sent to the Dragos OT Notifications feed above and are parsed according to the mapping table provided for that feed. The event description for type Alert is built using the parameters from the Notifications feed.

The event description is built using the following fields:

- `.id`
- `.hypothesis`

- `.justification`
- `.notes.author` (supplemental feed data)
- `.notes.message` (supplemental feed data)
- `.notes.updatedAt` (supplemental feed data)
- `.evidences.name` (supplemental feed data)
- `.evidences.snippet` (supplemental feed data)

The event title is built using the following fields (for Event Type: Alert):

- `.summary`
- `.severity` (Mapped according to severity mapping table)
- `.assets[0].attributes.host.name` (or `No Asset`)
- The length of `.assets` in case > 1
- value.id

ThreatQuotient provides the following default mapping for this feed based on each item within the API response's `.content` array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Event.Title	Event	.createdAt	`CobaltStrike Investigation`	Event Type: Case
Multiple fields listed above	Event.Title	Event	.assets[].createdAt	`New Ethernet Address as Source...`	Event Type: Alert
.assignee	Event.Attribute	Assignee	.createdAt	`N/A`	Updatable
.creator	Event.Attribute	Creator	.createdAt	`admin`	N/A
.incident	Event.Attribute	Type	.createdAt	`false`	'Incident' if True else 'Hunt'
.priority	Event.Attribute	Priority	.createdAt	`4`	Updatable
.status	Event.Attribute	Status	.createdAt	`OPEN`	Updatable
.visibility	Event.Attribute	Visibility	.createdAt	`PUBLIC`	Updatable
.watchersCount	Event.Attribute	Watchers Count	.createdAt	`0`	Updatable

Dragos OT Notifications

The Dragos OT Notifications feed ingests notifications along with the affected assets, discovered by Dragos OT. Notifications will be ingested as Event objects and will be related to the affected assets & MITRE ATT&CK techniques.

`GET https://{{ host }}/notifications/api/v2/notification`

Sample Response:


```
{
  "content": [
    {
      "analyticEventId": "597b1679c0b1def2ff6c0cf6dd7ec335",
      "analyticEventIndex": "tags",
      "assets": [
        {
          "addresses": [
            {
              "createdAt": "2025-04-01T08:32:09.399Z",
              "id": 586,
              "networkId": "89909de2-2dd5-4e3f-9120-79e3b0d0877b",
              "type": "MAC",
              "value": "FA:16:3E:4C:B5:42"
            },
            {
              "createdAt": "2025-04-01T08:32:09.407Z",
              "id": 587,
              "networkId": "89909de2-2dd5-4e3f-9120-79e3b0d0877b",
              "type": "IP",
              "value": "10.114.0.150"
            },
            {
              "createdAt": "2025-04-01T08:34:09.414Z",
              "id": 588,
              "networkId": "89909de2-2dd5-4e3f-9120-79e3b0d0877b",
              "type": "IP",
              "value": "FE80::F816:3EFF:FE4C:B542"
            }
          ],
          "attributes": {
            "host.address_id": [586, 587, 588],
            "host.domain": ["snapcraft.io"],
            "host.first_seen": "2025-04-01T08:31:15.191Z",
            "host.hostname": ["ladams-ms-test"],
            "host.id": "225",
            "host.ip": ["10.114.0.150", "FE80::F816:3EFF:FE4C:B542"],
            "host.last_seen": "2025-04-01T08:35:42.965Z",
            "host.mac": ["FA:16:3E:4C:B5:42"],
            "host.name": "Asset 225",
```

```
            "host.zone.id": 1,
            "host.zone.name": "RFC1918",
            "host.zone_id": 1,
            "labels.Monitored": "true",
            "observed.host.first_seen": "2025-04-01T08:31:15.191Z",
            "observed.host.last_seen": "2025-04-01T08:35:42.965Z",
            "observed.host.zone.id": 1,
            "observed.host.zone_id": 1,
            "observed.zoneId": 1,
            "related.network": ["89909de2-2dd5-4e3f-9120-79e3b0d0877b"],
            "related.observer": [
              "f594ad6e-5eff-4121-b581-d0443ed71caf",
              "7e0755ba-afa7-4fb1-a9d1-395eee6d5e9d"
            ],
            "tags": [
              "FileUpload"
            ],
            "zoneId": 1
          },
          "createdAt": "2025-04-01T08:31:15.191Z",
          "directionalities": ["source"],
          "enriched": true,
          "id": 225
        }
      ],
      "collectors": [
        {
          "collectorId": "collectorbond",
          "customerId": "default",
          "sensorId": "f594ad6e-5eff-4121-b581-d0443ed71caf"
        }
      ],
      "content": "Asset:225 (FA:16:3E:4C:B5:42) seen as the ethernet source for
the first time",
      "count": 1,
      "createdAt": "2025-04-01T08:45:38Z",
      "detectionQuads": ["Configuration"],
      "detectorId": "0f6881dd-fd83-4e34-968f-a8c08aab07cf",
      "firstSeenAt": "2025-04-01T08:32:18Z",
      "id": 1236,
      "lastSeenAt": "2025-04-01T08:32:18Z",
      "matchedRuleIds": [],
      "occurredAt": "2025-04-01T08:32:18Z",
      "retained": false,
      "reviewed": false,
      "severity": 1,
      "source": "0a437c95-a984-40b1-b1a0-f96a32375ff5",
      "sourceIdField": "uuid",
      "sourceIds": ["0a437c95-a984-40b1-b1a0-f96a32375ff5"],
      "sourceIndex": "pipeline",
```

```
      "state": "UNRESOLVED",
      "summary": "New Ethernet Address as Source",
      "threatInfo": [
        {
          "framework": "MITRE ATTCK FOR ICS",
          "tactic": {
            "id": "TA0011",
            "name": "Command and Control",
            "reference": "https://attack.mitre.org/tactics/TA0011"
          },
          "technique": {
            "id": "T1105",
            "name": "Ingress Tool Transfer",
            "reference": "https://attack.mitre.org/techniques/T1105"
          }
        }
      ],
      "type": "Communication"
    }
  ],
  "pageNumber": 1,
  "pageSize": 100,
  "sorts": [
    {
      "descending": false,
      "field": "createdAt"
    }
  ],
  "totalCount": 1,
  "totalPages": 1
}
```


The event description is built using the following fields:

- `.assets[].id`
- `.assets[].content`
- `.assets[].firstSeenAt`
- `.assets[].occurredAt`
- `.assets[].lastSeenAt`
- `.assets[].createdAt`
- `.assets[].threatInfo[].technique.reference`
- `.assets[].threatInfo[].technique.id`
- `.assets[].threatInfo[].technique.name`
- `.assets[].threatInfo[].tactic.name`
- `.assets[].attributes.host.name`
- `.assets[].attributes.host.zone.name`
- `.assets[].attributes.host.mac[]`
- `.assets[].attributes.host.ip[]`
- `.assets[].attributes.host.domain[]`
- `.assets[].attributes.host.hostname[]`

- `.assets[].attributes.tags[]`
- `.assets[].attributes.host.first_seen`
- `.assets[].attributes.host.last_seen`

The event title is built using the following fields:

- `.summary`
- `.severity` (Mapped according to severity mapping table)
- `.assets[0].attributes.host.name` (or `No Asset`)
- The length of `.assets` in case > 1
- `value.id`

ThreatQuotient provides the following default mapping for this feed based on each item within the API response's `.content` array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
Multiple fields listed above	Event.Title	Event	.assets[].createdAt	`New Ethernet Address as Source...`	N/A
.assets[].attributes.tags[]	Event.Tags	N/A	N/A	`FileUpload`	User-configurable
.assets[].threatInfo[].tactic.name	Event.Tags	N/A	N/A	`Command and Control`	User-configurable
.assets[].state	Event.Attribute	State	.assets[].createdAt	`UNRESOLVED`	Updatable
.assets[].source	Event.Attribute	Source	.assets[].createdAt	`0a437c95-a984-40b1-b1a0-f96a32375ff5`	User-configurable
.assets[].count	Event.Attribute	Count	.assets[].createdAt	`1`	User-configurable. Updatable
.assets[].severity	Event.Attribute	Severity	.assets[].createdAt	`Low`	User-configurable. Mapped according to severity mapping table. Updatable
.assets[].severity	Event.Attribute	Severity Score	.assets[].createdAt	`1`	User-configurable. Updatable
.assets[].detectionQuads	Event.Attribute	Detection Type	.assets[].createdAt	`Configuration`	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.assets[].type	Event.Attribute	Notification Type	.assets[].createdAt	`Communication`	User-configurable
.assets[].reviewed	Event.Attribute	Is Reviewed	.assets[].createdAt	`false`	User-configurable. Boolean. Updatable
.assets[].retained	Event.Attribute	Is Retained	.assets[].createdAt	`false`	User-configurable. Boolean. Updatable
.assets[].attributes.host.id	Related Asset.Value	Asset	N/A	`Asset 225`	User-configurable. Appended with "Asset" to form the name
.assets[].attributes.host.zone.name	Related Asset.Attribute	Zone	.assets[].attributes.host.first_seen	`RFC1918`	Updatable
.assets[].attributes.host.name	Related Asset.Attribute	Name	.assets[].attributes.host.first_seen	`Asset 225`	Updatable
.assets[].attributes.host.mac[]	Related Asset.Attribute	Mac Address	.assets[].attributes.host.first_seen	`FA:16:3E:4C:B5:42`	Updatable
.assets[].attributes.host.ip[]	Related Asset.Attribute	IP Address	.assets[].attributes.host.first_seen	`10.114.0.150`	N/A
.assets[].attributes.host.ip[]	Related Asset.Attribute	IPv6 Address	.assets[].attributes.host.first_seen	`10.114.0.150`	N/A
.assets[].attributes.host.domain[]	Related Asset.Attribute	Domain	.assets[].attributes.host.first_seen	`snapcraft.io`	N/A
.assets[].attributes.host.hostname[]	Related Asset.Attribute	Hostname	.assets[].attributes.host.first_seen	`ladams-ms-test`	N/A
.assets[].attributes.host.first_seen	Related Asset.Attribute	First Seen	.assets[].attributes.host.first_seen	`2025-04-01T08:31:15.191Z`	Updatable
.assets[].attributes.host.last_seen	Related Asset.Attribute	Last Seen	.assets[].attributes.host.first_seen	`2025-04-01T08:35:42.965Z`	Updatable
.content	Related Indicator/ Vulnerability.Value	Multiple Types/ Vulnerability	.assets[].createdAt	`N/A`	Parsed from content. CVEs are user configurable
.assets[].severity	Related Indicator/ Vulnerability.Attribute	Severity	.assets[].createdAt	`Low`	Mapped according to severity mapping table
.assets[].threatInfo[].technique.name	Related Attack Pattern.Value	Attack Pattern	.assets[].createdAt	`T1105 - Ingress`	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				`Tool` `Transfer`	

Severity Mapping

The following mapping illustrates how Dragos Severity values are mapping in ThreatQ.

DRAGOS SEVERITY	THREATQ SEVERITY
0	`Informational`
1	`Low`
2	`Medium`
3	`High`
4	`Very High`
5	`Critical`

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.

Dragos OT Cases

METRIC	RESULT
Run Time	1 minute
Assets	2
Attack Patterns	1
Events	8
Event Attributes	45

Dragos OT Notifications

METRIC	RESULT
Run Time	1 minute
Attack Patterns	4
Assets	3
Events	12
Event Attributes	60
Indicators	2

Change Log

- **Version 1.0.0**
  - Initial release