ThreatQuotient

A Securonix Company

Dragos CDF

Version 2.0.2

June 15, 2026

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

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: 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

Current Integration Version	2.0.2
Compatible with ThreatQ Versions	>= 6.6.0
Support Tier	ThreatQ Supported

Introduction

The Dragos CDF integration allows teams to seamlessly ingest Dragos WorldView Product Reports and Indicators into ThreatQ. Leveraging the Dragos WorldView API, the integration delivers comprehensive intelligence on threats targeting industrial control systems (ICS) and operational technology (OT) environments.

The integration provides the following feeds:

- **Dragos Product Reports** - fetches, parses, and ingests Dragos Product Reports, which include threat intelligence on industrial control systems (ICS) and operational technology (OT) environments.
- **Dragos Indicators** - fetches curated tactical indicators impacting ICS and OT environments, from Dragos's API.

The integration ingests the following object types:

- Adversaries
- Attack Patterns
- Indicators
- Intel Requirements (Custom Object)
- Malware
- Reports
- Vulnerabilities

Prerequisites

The following is required in order to install and run the integration:

- A Dragos API Key and Token from the Dragos WorldView portal.
- Optional - Intel Requirement custom object installed.

> This Intel Requirement custom object is required if you choose to ingest intel requirements as Intel Requirement objects as opposed to Attributes for the Dragos Product Reports feed. This is configured via the **Ingest Intel Requirements As** parameter.

Intel Requirement Custom Object

The integration requires the Intel Requirement custom object if Intel Requirements are configured to be ingested as Intel Requirement objects rather than attributes - see the **Ingest Intel Requirements As** parameter.

Use the steps provided to install the Intel Requirement custom object.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Set your install pathway environment variable. This command will retrieve the install pathway from your configuration file and set it as variable for use during this installation process.

```
INSTALL_CONF="/etc/threatq/platform/install.conf"

if [ -f "$INSTALL_CONF" ]; then source "$INSTALL_CONF"

fi
```

```
MISC_DIR="${INSTALL_BASE_PATH:-/var/lib/threatq}/misc"
```

5. Navigate to the tmp folder using the environment variable:

```
cd $MISC_DIR
```

6. Upload the custom object files, including the images folder.

   The directory structure should resemble the following:

   - install.sh
   - <custom_object_name>.json
   - images (directory)
     - <custom_object_name>.svg

7. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq --
sh /var/lib/threatq/misc/install.sh /var/lib/threatq/misc
```

   The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

8. Delete the install.sh, definition json file, and images directory from step 6 after the object has been installed as these files are no longer needed.

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 zip file.
3. Extract the contents of the zip file and install the Intel Requirement custom object if you plan to ingest Intel Requirements data into the platform as objects - see Intel Requirements section for more details.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration yaml file.
7. Select the individual feeds to install and click **Install**.

The feed(s) will be added to the integrations page. You will still need to configure and enable the feeds.

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** category from the Category dropdown.
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Dragos Product Reports

PARAMETER	DESCRIPTION
API Access Token	Enter your Dragos API Token.
API Secret Key	Enter your Dragos API Secret Key
Ingest CVEs As	Select how to ingest CVEs as in the ThreatQ platform. Options include as **Vulnerabilities** (default) or **Indicators** (type: CVE)
Ingest Intel Requirements As	Select how to ingest Intel Requirements. Options include as **Attributes** (default) or as **Intel Requirement Objects**. You must have the Intel Requirement custom object installed if you select `Intel Requirement Objects` option.
I Have the Intel Requirement Custom Object Installed	Enable this checkbox to confirm that you have installed the Intel Requirement custom object.

PARAMETER	DESCRIPTION
	This confirmation checkbox will only be accessible if you have selected the `Intel Requirement Objects` option for the Ingest **Intel Requirements As** parameter.
API Delay	Enter a delay, in seconds, between supplemental API requests. This will help avoid hitting rate limits. The default value is 1.
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.

Dragos Indicators

PARAMETER	DESCRIPTION
API Access Token	Enter your Dragos API Token.
API Secret Key	Enter your Dragos API Secret Key
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.

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 Product Reports

The Dragos Product Reports feed fetches, parses, and ingests Dragos Product Reports, which include threat intelligence on industrial control systems (ICS) and operational technology (OT) environments.

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

Sample Response:


```
{
  "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
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Report.Value	N/A	.updated_at	WorldView Special - 04212017 - NYC/ SFO Power Outages	N/A
.executive_summary	Report.Description	N/A	.updated_at	On 21 April 2017 two separate power outages...	N/A
.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
.type	Report.Attribute	Report Type	.updated_at	WorldView Special	N/A
.report_link	Report.Attribute	Report Link	.updated_at	https://portal.dragos.com/api/v1/products/WVS-2017-02/report	N/A
.threat_level	Report.Attribute	Threat Level	.updated_at	Low	Converted from integer to value according to this mapping:(0: Low, 1: Medium, 2: High, 3: Very High, 4: Critical)
.serial	Report.Attribute	Identifier	.updated_at	WVS-2017-02	N/A
.tags[].text	Report.Attribute	<tag type>	.updated_at	Location: Europe	Tags are parsed into attributes based on their type, and the Intel Requirement ID is ingested as an attribute when the *Ingest Intel Requirements As* user configuration is set for *Attributes*.
.tags[].text	Report.Adversary	N/A	.updated_at	BAUXITE	Tags are parsed for adversaries based on the tag type (ThreatGroup, HackerGroup, ExternalName)

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.tags[].text	Report.AttackPattern	N/A	.updated_at	T1583 - Acquire Infrastructure	Tags are parsed for Attack Patterns based on the tag type (ATT&CK Technique). See note below on Attack Patterns.
.tags[].text	Report.Vulnerability, Report.Indicator	CVE	.updated_at	CVE-2017-0144	Tags are parsed for Vulnerabilities/ Indicators based on the tag type (CVE)
.tags[].text	Report.Malware	N/A	.updated_at	Cobalt Strike	Tags are parsed for Malware based on the tag type (Ransomware)
.tags[].text	Report.IntelRequirement	N/A	.updated_at	IR-2024-02 - <name>	User Configurable. Tags are parsed for Intel Requirements based on the tag type (Intel Requirement). The IDs will be ingested as attributes if the Intel Requirement custom object is not installed. The custom object must be installed if 'Ingest Intel Requirements As' user configuration is set on Intel Requirement Objects, and Ingest Intel Requirement Object Confirmation is checked.
.tags[].text	Report.Tag	N/A	.updated_at	APT	Tags that do not have a tag type will be ingested as a Tag instead of an Attribute.

Dragos to ThreatQ Report Additional Mapping

DRAGOS VALUE	THREATQ VALUE
GeographicLocation	Location
Product	Affected Product
Vendor	Affected Vendor
Port	Port Info
Industry	Target Industry
KillChain	Kill Chain Phase

Notes

- If `.ioc_count` is non-zero, a supplemental call to the Dragos Indicators endpoint is made to fetch Indicators based on .serial related to the Report.

- The mapping for the Indicators is provided in the Dragos Indicators section below.
- Tactics (Attributes), Techniques (Attack Patterns), Adversaries, and Kill Chain Phases are parsed from related indicators and also from .tags[] for the Report.
- Attack Patterns are parsed from `.tags[]` if `.tags[].tag_type` is ATT&CK Technique. Below is shown how this type of tag can be present in the API's response. If the `.text` contains the full name of an attack pattern (T - <VALUE>), the corresponding attack pattern is related to the report, otherwise the name of the technique (Phishing in the example below) is related to the report.

```
{
  "tags": [
    {
      "text": "Initial Access:Phishing",
      "tag_type": "ATT&CK Technique"
    },
    {
      "text": "T1572 - Protocol Tunneling",
      "tag_type": "ATT&CK Technique"
    }
  ]
}
```

Dragos Indicators

The Dragos Indicators feed fetches curated tactical indicators impacting ICS and OT environments, from Dragos's API.

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

Sample Response:


```
{
  "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
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value	Indicator.Value	Mapping using Indicator Mapping based on the value of .indicator_type	.first_seen	167.114.213.199	N/A
.category	Indicator.Attribute	Category	.first_seen	Network activity	N/A
.status	Indicator.Attribute	Status	.first_seen	released	N/A
.confidence	Indicator.Attribute	Confidence	.first_seen	moderate	N/A
.kill_chain	Indicator.Attribute	Kill Chain Phase	.first_seen	Exploit	The Stage number is stripped from the value to better align with ThreatQ's terminology
.severity	Indicator.Attribute	Severity	.first_seen	2	N/A
.comment	Indicator.Attribute	Comment	.first_seen	N/A	N/A
.attack_techniques[], .ics_attack_techniques[], .pre_attack_techniques[]	Indicator.Attribute	Tactic	.first_seen	Reconnaissance	Tactic is extracted from MITRE Technique value
.activity_groups[], .threat_groups[]	Indicator.Adversary	N/A	N/A	ALLANITE	N/A
.attack_techniques[], .ics_attack_techniques[], .pre_attack_techniques[]	Indicator.AttackPattern	N/A	.first_seen	Initial Access:Supply Chain Compromise	The name of the technique is mapped to an existing ThreatQ Attack Pattern

Dragos Indicators to ThreatQ Mapping

The follow table shows how Dragos indicator types are mapped in ThreatQ.

DRAGOS TYPE	THREATQ INDICATOR TYPE
ip	IP Address

DRAGOS TYPE	THREATQ INDICATOR TYPE
domain	FQDN
md5	MD5
sha1	SHA-1
sha56	SHA-256

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 Product Reports

METRIC	RESULT
Run Time	1 minute
Adversaries	11
Attack Patterns	15
Indicators	428
Indicator Attributes	1,713
Malware	1
Reports	10
Report Attributes	145

Dragos Indicators

METRIC	RESULT
Run Time	53 minutes
Adversaries	13
Attack Patterns	38
Indicators	17,210
Indicator Attributes	57,476

Known Issues / Limitations

- MITRE ATT&CK Attack Patterns must have already been ingested by MITRE ATT&CK feeds in order to be related to Indicators. The following feeds ingest MITRE ATT&CK Attack Patterns:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE ISC ATT&CK

Change Log

- **Version 2.0.2**
  - Updated Dragos indicator severity handling to preserve API-provided severity values, including integer-based severities, preventing ingestion failures and improving compatibility with Dragos data.
- **Version 2.0.1**
  - Optimized MITRE ATT&CK technique mapping initialization for Dragos Product Reports by relocating it outside of the per-indicator processing loop, reducing the risk of timeouts when handling related indicators.
- **Version 2.0.0 rev-a**
  - Guide Update - updated custom object installation steps for ThreatQ v6 instances.
- **Version 2.0.0**
  - The **Dragos Products** feed has been renamed to **Dragos Product Reports**.
  - Tags are now parsed for related Malware, Adversaries, Attack Patterns (MITRE ATT&CK Techniques), and Vulnerabilities (CVEs).
  - The `Kill Chain` attribute has been renamed to `Kill Chain Phase`.
  - Users can now leverage the Intel Requirement Custom Object to ingest relevant intel requirements from Dragos Product Reports.

    Intel Requirements can also be ingested as attributes (ID only).
  - The following attributes have been renamed to better align with ThreatQ's terminology:
    - `Product` has been renamed to `Affected Product`
    - `Vendor` has been renamed to `Affected Vendor`
    - `Port` has been renamed to `Port Info`
    - `GeographicLocation` has been renamed to `Location`
    - `Industry` has been renamed to `Target Industry`
  - The `Port` attribute has been renamed to `Port Info` to better reflect its contents.
  - Added support for pagination when fetching Dragos Indicators.

- Improved handling of Dragos API rate limits, including a delay of 60 seconds before retrying after a 429 error.
- Updated the integration to the latest set of standards while incorporating new features and improvements.
- Updated the minimum ThreatQ version to 6.6.0.

- **Version 1.0.0**
  - Initial release