ThreatQuotient

Intel 471 GIRs CDF

Version 1.0.0

November 18, 2024

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

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Intel Requirement Custom Object 7
ThreatQ V6 Steps 7
ThreatQ v5 Steps 8
Installation **10**
Configuration **11**
ThreatQ Mapping **12**
Intel 471 GIRs 12
Average Feed Run **14**
Change Log **15**

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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Intel 471 GIRs integration provides a feed of Intel 471's Generalized Intelligence Requirements (GIRs) into ThreatQ, using the Intel Requirement custom object type.

The integration provides the following feed:

- **Intel 471 GIRs** - ingests Intel 471's GIRs into the ThreatQ platform as Intel Requirement objects.

The integration ingests the Intel Requirement custom object into the ThreatQ platform.

Prerequisites

The integration requires the installation of the Intel Requirement custom object.

Intel Requirement Custom Object

The integration requires the Intel Requirement custom object.

Use the steps provided to install the 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.

ThreatQ V6 Steps

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. Navigate to the tmp folder:

   ```
   cd /var/lib/threatq/misc/
   ```

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

   The directory structure should be as the following:

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

6. 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.

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

ThreatQ v5 Steps

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir intel471_cdf
   ```

5. Upload the **intel_requirement.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the intel471_cdf directory.

   ```
   mkdir images
   ```

7. Upload the intel_requirement.svg.
8. Navigate to the **/tmp/intel471_cdf**.

   The directory should resemble the following:

   - tmp
     - **intel471_cdf**
       - **intel_requirement.json**
       - **install.sh**
       - **images**
         - **intel_requirement.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

   ```
   chmod +x install.sh
   ```

10. Run the following command:

    ```
    sudo ./install.sh
    ```

    > You must be in the directory level that houses the install.sh and json files when running this command.

    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.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf intel471_cdf
```

Installation

The CDF requires the installation of Intel Requirement custom object before installing the actual CDF. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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 and install the Intel Requirement custom object if you have not done so already.
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 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
7. 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. Review any feed settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Intel 471 GIRs

The Intel 471 GIRs feed ingests Intel 471 GIRs into the ThreatQ platform as Intel Requirement custom objects.

`GET https://raw.githubusercontent.com/intel471/CU-GIR/main/STIX/Current/intel471_cu-gir.json`

Sample Response:


```
[
  {
    "type": "attack-pattern",
    "spec_version": "2.1",
    "created": "15/06/2023 09:49:18",
    "modified": "15/06/2023 09:49:18",
    "id": "attack-pattern--90efbe2f-61fa-4b54-a4b0-cdb419f492c5",
    "name": "Wholesale access",
    "description": "Purported access to a network, resource or service by means of compromised access credentials, exploitation of a software vulnerability or misconfiguration or via similar means for which no indicator exists that a threat actor verified the validity of access as operational.",
    "aliases": null,
    "kill_chain_phases": [],
    "external_references": [],
    "x_gir_id": "4.7.1",
    "x_deprecated": false
  },
  {
    "type": "identity",
    "spec_version": "2.1",
    "created": "12/06/2023 13:54:25",
    "modified": "12/06/2023 13:54:25",
    "id": "identity--c5e2b26d-96b1-ce5f-bebc-531591027c07",
    "name": "Cryptocurrency industry",
    "description": "",
    "identity_class": null,
    "contact_information": null,
    "roles": null,
    "sectors": null,
    "x_gir_id": "6.1.13.1",
    "x_deprecated": false
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.x_gir_id`, `.name`	Intel Requirement	N/A	N/A	`6.1.13.1 - Cryptocurrent industry`	N/A
`.description`	Description	N/A	N/A	N/A	N/A

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.

METRIC	RESULT
Run Time	1 minute
Intel Requirements	480

Change Log

- **Version 1.0.0**
  - Initial release