ThreatQuotient

ThreatQ STIX 2.1 Exporter Operation Guide

Version 1.0.0

November 10, 2021

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

Not Supported

Contents

Support **4**
Versioning **5**
Introduction **6**
Installation **7**
Configuration **8**
Actions **9**
Create Bundle 10
Parameters 10
Sample Output Bundle 11
Create Sighting 14
Parameters 14
Sample Output Bundle 15
Known Issues / Limitations **18**
Change Log **19**

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 **Not Supported**.

Integrations, apps, and add-ons designated as **Not Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Supported integrations/apps/add-ons.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.35`

Introduction

The STIX 2.1 Exporter Operation for ThreatQ enables an analyst to export an object and its' relationships to STIX 2.1 JSON.

The integration's actions are compatible with the following object types:

- Adversary
- Attack Pattern
- Campaign
- Course of Action
- Event
- Exploit Target
- Identity
- Incident
- Indicator
- Intrusion Set
- Malware
- Tool

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
Convert Events to Incident Objects	Enabling this will convert related event objects to STIX 2.1 Incident objects.
Hostname	(Optional) Your ThreatQ hostname or IP address for creating links back to this instance.

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

Actions

ACTION	DESCRIPTION	OBJECT TYPES
Create Bundle	Create a STIX 2.1 bundle from an object and its' relationships.	Indicator, Adversary, Attack Pattern, Campaign, Malware, Course of Action, Exploit Target, Intrusion Set, Incident, Tool, Identity
Create Sighting	Create a STIX 2.1 sighting from an object and its' relationships.	Indicator, Incident, Event

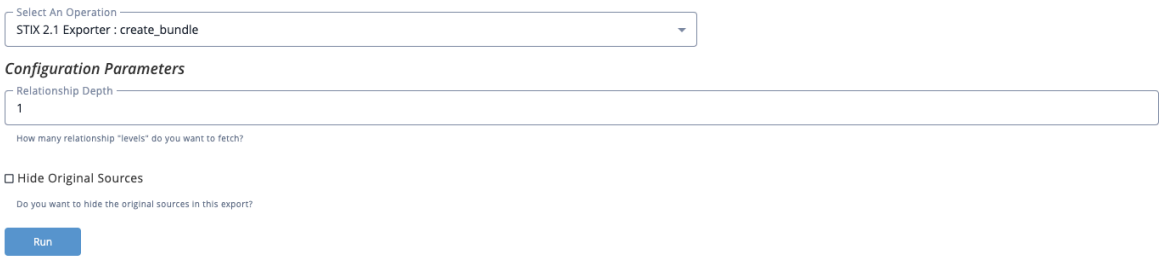
Create Bundle

The Create Bundle action creates a STIX 2.1 bundle from an Object and its' relationships.

Parameters

When selecting the action, you will be prompted with the following parameters:

PARAMETER	DESCRIPTION
Relationships Depth	Set how many relationship levels to fetch. The max setting is 3.
Hide Original Sources	Use the checkbox to select if the original sources will be hidden in the export. This parameter is unchecked by default.



Sample Output Bundle

Below is a sample output JSON file containing the STIX 2.1 bundle. This bundle will be uploaded and related as a File in ThreatQ.


```
{
    "id": "bundle--d4882900-5a35-4c75-af9c-06eb6e43d6f3",
    "objects": [
        {
            "created": "2021-10-07T14:19:15.000Z",
            "external_references": [
                {
                    "description": "Intelligence exported from ThreatQ",
                    "source_name": "ThreatQ"
                },
                {
                    "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                    "source_name": "CrowdStrike Insight EDR - Detections"
                }
            ],
            "id": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
            "modified": "2021-10-07T14:19:54.000Z",
            "name": "High Severity Detection on WIN10DETECTION - ldt:4c3db6145a704a179a6dacd924f6e8cc:68731692068",
            "spec_version": "2.1",
            "type": "incident"
        },
        {
            "created": "2021-10-07T14:05:58.000Z",
            "external_references": [
                {
                    "description": "Intelligence exported from ThreatQ",
                    "source_name": "ThreatQ"
                },
                {
                    "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                    "source_name": "CrowdStrike Insight EDR - Detections"
                }
            ],
            "id": "indicator--5c66c742-b2f4-4b6b-8d15-92142cc5aac4",
            "modified": "2021-10-07T14:19:58.000Z",
            "name": "123328fe9a690ad5854c9e6d37ffbb38cd35af0e39c9b35e8567e914cdab266f",
            "pattern": "[file:hashes.'SHA-256' =
'123328fe9a690ad5854c9e6d37ffbb38cd35af0e39c9b35e8567e914cdab266f']",
            "pattern_type": "stix",
            "pattern_version": "2.1",
            "spec_version": "2.1",
            "type": "indicator",
            "valid_from": "2021-10-07T14:05:58Z"
        },
        {
            "created": "2021-10-21T21:02:46.435848Z",
            "id": "relationship--8bf2b521-6791-48d3-a7fd-4fc9d3d61cd2",
            "modified": "2021-10-21T21:02:46.435848Z",
            "relationship_type": "related-to",
            "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
            "spec_version": "2.1",
```

```
        "target_ref": "indicator--5c66c742-b2f4-4b6b-8d15-92142cc5aac4",
        "type": "relationship"
    },
    {
        "created": "2021-10-07T14:05:58.000Z",
        "external_references": [
            {
                "description": "Intelligence exported from ThreatQ",
                "source_name": "ThreatQ"
            },
            {
                "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                "source_name": "CrowdStrike Insight EDR - Detections"
            }
        ],
        "id": "indicator--c4e904e9-884d-46f2-9f3c-c2adddcf9fff",
        "modified": "2021-10-07T14:19:58.000Z",
        "name": "3b35d89b10e561e05006e0a101154348",
        "pattern": "[file:hashes.'MD5' = '3b35d89b10e561e05006e0a101154348']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "spec_version": "2.1",
        "type": "indicator",
        "valid_from": "2021-10-07T14:05:58Z"
    },
    {
        "created": "2021-10-21T21:02:46.436108Z",
        "id": "relationship--577e3b8b-5a97-4cf0-914f-7ba9677c1923",
        "modified": "2021-10-21T21:02:46.436108Z",
        "relationship_type": "related-to",
        "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
        "spec_version": "2.1",
        "target_ref": "indicator--c4e904e9-884d-46f2-9f3c-c2adddcf9fff",
        "type": "relationship"
    },
    {
        "created": "2021-10-07T14:05:58.000Z",
        "external_references": [
            {
                "description": "Intelligence exported from ThreatQ",
                "source_name": "ThreatQ"
            },
            {
                "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                "source_name": "CrowdStrike Insight EDR - Detections"
            }
        ],
        "id": "attack-pattern--de1a0a82-dc07-44d8-ba5b-11ecf5a37cf9",
        "modified": "2021-10-07T14:19:58.000Z",
        "name": "CST0005 - Indicator of Compromise",
        "spec_version": "2.1",
        "type": "attack-pattern"
    },
    {
        "created": "2021-10-21T21:02:46.437427Z",
        "id": "relationship--29c7452d-edac-4a54-8185-5bdafec27d5f",
        "modified": "2021-10-21T21:02:46.437427Z",
        "relationship_type": "related-to",
        "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
        "spec_version": "2.1",
```

```
            "target_ref": "attack-pattern--de1a0a82-dc07-44d8-ba5b-11ecf5a37cf9",
            "type": "relationship"
        },
        {
            "created": "2021-10-07T14:05:58.000Z",
            "external_references": [
                {
                    "description": "Intelligence exported from ThreatQ",
                    "source_name": "ThreatQ"
                },
                {
                    "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                    "source_name": "CrowdStrike Insight EDR - Detections"
                }
            ],
            "id": "attack-pattern--a4314d5f-7906-47d0-8829-ffcff84e939b",
            "modified": "2021-10-07T14:19:58.000Z",
            "name": "CST0008 - Cloud-based ML",
            "spec_version": "2.1",
            "type": "attack-pattern"
        },
        {
            "created": "2021-10-21T21:02:46.437647Z",
            "id": "relationship--5007d994-91ac-4a0e-8a6b-752447ff4e86",
            "modified": "2021-10-21T21:02:46.437647Z",
            "relationship_type": "related-to",
            "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
            "spec_version": "2.1",
            "target_ref": "attack-pattern--a4314d5f-7906-47d0-8829-ffcff84e939b",
            "type": "relationship"
        }
    ],
    "type": "bundle"
}
```

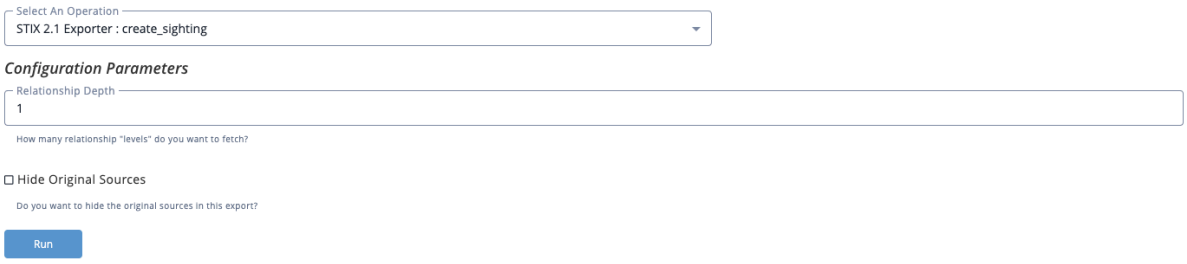
Create Sighting

Create a STIX 2.1 sighting from an Object and its' relationships

Parameters

When selecting the action, you will be prompted with the following parameters:

PARAMETER	DESCRIPTION
Relationships Depth	Set how many relationship levels to fetch. The max setting is 3.
Hide Original Sources	Use the checkbox to select if the original sources will be hidden in the export. This parameter is unchecked by default.



Sample Output Bundle

Below is a sample output JSON file containing the STIX 2.1 bundle. This bundle will be uploaded and related as a File in ThreatQ.


```
{
    "id": "bundle--d4882900-5a35-4c75-af9c-06eb6e43d6f3",
    "objects": [
        {
            "created": "2021-10-07T14:19:15.000Z",
            "external_references": [
                {
                    "description": "Intelligence exported from ThreatQ",
                    "source_name": "ThreatQ"
                },
                {
                    "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                    "source_name": "CrowdStrike Insight EDR - Detections"
                }
            ],
            "id": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
            "modified": "2021-10-07T14:19:54.000Z",
            "name": "High Severity Detection on WIN10DETECTION - ldt:4c3db6145a704a179a6dacd924f6e8cc:68731692068",
            "spec_version": "2.1",
            "type": "incident"
        },
        {
            "created": "2021-10-07T14:05:58.000Z",
            "external_references": [
                {
                    "description": "Intelligence exported from ThreatQ",
                    "source_name": "ThreatQ"
                },
                {
                    "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                    "source_name": "CrowdStrike Insight EDR - Detections"
                }
            ],
            "id": "indicator--5c66c742-b2f4-4b6b-8d15-92142cc5aac4",
            "modified": "2021-10-07T14:19:58.000Z",
            "name": "123328fe9a690ad5854c9e6d37ffbb38cd35af0e39c9b35e8567e914cdab266f",
            "pattern": "[file:hashes.'SHA-256' =
'123328fe9a690ad5854c9e6d37ffbb38cd35af0e39c9b35e8567e914cdab266f']",
            "pattern_type": "stix",
            "pattern_version": "2.1",
            "spec_version": "2.1",
            "type": "indicator",
            "valid_from": "2021-10-07T14:05:58Z"
        },
        {
            "created": "2021-10-21T21:02:46.435848Z",
            "id": "relationship--8bf2b521-6791-48d3-a7fd-4fc9d3d61cd2",
            "modified": "2021-10-21T21:02:46.435848Z",
            "relationship_type": "related-to",
            "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
            "spec_version": "2.1",
```

```
        "target_ref": "indicator--5c66c742-b2f4-4b6b-8d15-92142cc5aac4",
        "type": "relationship"
    },
    {
        "created": "2021-10-07T14:05:58.000Z",
        "external_references": [
            {
                "description": "Intelligence exported from ThreatQ",
                "source_name": "ThreatQ"
            },
            {
                "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                "source_name": "CrowdStrike Insight EDR - Detections"
            }
        ],
        "id": "indicator--c4e904e9-884d-46f2-9f3c-c2adddcf9fff",
        "modified": "2021-10-07T14:19:58.000Z",
        "name": "3b35d89b10e561e05006e0a101154348",
        "pattern": "[file:hashes.'MD5' = '3b35d89b10e561e05006e0a101154348']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "spec_version": "2.1",
        "type": "indicator",
        "valid_from": "2021-10-07T14:05:58Z"
    },
    {
        "created": "2021-10-21T21:02:46.436108Z",
        "id": "relationship--577e3b8b-5a97-4cf0-914f-7ba9677c1923",
        "modified": "2021-10-21T21:02:46.436108Z",
        "relationship_type": "related-to",
        "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
        "spec_version": "2.1",
        "target_ref": "indicator--c4e904e9-884d-46f2-9f3c-c2adddcf9fff",
        "type": "relationship"
    },
    {
        "created": "2021-10-07T14:05:58.000Z",
        "external_references": [
            {
                "description": "Intelligence exported from ThreatQ",
                "source_name": "ThreatQ"
            },
            {
                "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                "source_name": "CrowdStrike Insight EDR - Detections"
            }
        ],
        "id": "attack-pattern--de1a0a82-dc07-44d8-ba5b-11ecf5a37cf9",
        "modified": "2021-10-07T14:19:58.000Z",
        "name": "CST0005 - Indicator of Compromise",
        "spec_version": "2.1",
        "type": "attack-pattern"
    },
    {
        "created": "2021-10-21T21:02:46.437427Z",
        "id": "relationship--29c7452d-edac-4a54-8185-5bdafec27d5f",
        "modified": "2021-10-21T21:02:46.437427Z",
        "relationship_type": "related-to",
        "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
        "spec_version": "2.1",
```

```
            "target_ref": "attack-pattern--de1a0a82-dc07-44d8-ba5b-11ecf5a37cf9",
            "type": "relationship"
        },
        {
            "created": "2021-10-07T14:05:58.000Z",
            "external_references": [
                {
                    "description": "Intelligence exported from ThreatQ",
                    "source_name": "ThreatQ"
                },
                {
                    "description": "Intelligence reported by CrowdStrike Insight EDR - Detections",
                    "source_name": "CrowdStrike Insight EDR - Detections"
                }
            ],
            "id": "attack-pattern--a4314d5f-7906-47d0-8829-ffcff84e939b",
            "modified": "2021-10-07T14:19:58.000Z",
            "name": "CST0008 - Cloud-based ML",
            "spec_version": "2.1",
            "type": "attack-pattern"
        },
        {
            "created": "2021-10-21T21:02:46.437647Z",
            "id": "relationship--5007d994-91ac-4a0e-8a6b-752447ff4e86",
            "modified": "2021-10-21T21:02:46.437647Z",
            "relationship_type": "related-to",
            "source_ref": "incident--e583e41d-f0fb-41f2-a0e0-4be063713bda",
            "spec_version": "2.1",
            "target_ref": "attack-pattern--a4314d5f-7906-47d0-8829-ffcff84e939b",
            "type": "relationship"
        }
    ],
    "type": "bundle"
}
```

Known Issues / Limitations

STIX 2.1 Indicator/Observable objects can have multiple "indicators" associated with them so external references will **not** contain a URL back to the ThreatQ platform.

Change Log

- **Version 1.0.0**
  - Initial release