ThreatQuotient

ThreatQ STIX 2.1 Exporter Operation

Version 1.1.3

May 12, 2025

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

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	1.1.3
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported

Introduction

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

The operation includes the following actions:

- **Create Bundle** - creates a STIX 2.1 bundle from an object and its relationships.
- **Create Sighting** - creates a STIX 2.1 sighting from an object and its relationships.

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
- Report
- Tool
- Vulnerability

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 whl 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 operation 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.

The operation is now installed and will be displayed in the ThreatQ UI. 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).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Convert Events to Which Object	Select the STIX object type to convert events to or to ignore events.
Hostname	Optional- Your ThreatQ hostname or IP address for creating links back to this instance.

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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
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	N/A
Create Sighting	Create a STIX 2.1 sighting from an object and its' relationships.	Indicator, Incident, Event	N/A

Create Bundle

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

Action 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 2.
TLP Selection	Use the checkboxes to select which TLP designations to include with the STIX bundle. All options are selected by default.
Hide Original Sources	Use the checkbox to select if the original sources will be hidden in the export. This parameter is unchecked by default.

Select An Operation
STIX 2.1 Exporter : create_bundle

Configuration Parameters

Relationship Depth
1

How many relationship "levels" do you want to fetch?

TLP Selection

Select the TLP markings you want to include in your STIX Bundle

☑ Red

☑ Amber

☑ Green

☑ White

☑ Not Specified

☐ Hide Original Sources

Do you want to hide the original sources in this export?

Run

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.

Action 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 2.
Hide Original Sources	Use the checkbox to select if the original sources will be hidden in the export. This parameter is unchecked by default.

Select An Operation
STIX 2.1 Exporter : create_sighting

Configuration Parameters

Relationship Depth
1

How many relationship "levels" do you want to fetch?

☐ Hide Original Sources

Do you want to hide the original sources in this export?

Run

Sample Output Sighting

Below is a sample output JSON file containing the STIX 2.1 sighting. This sighting 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 1.1.3**
    - Resolved an issue where customers encountered an `Operation Setup Failure` error when attempting to install the operation in an air-gapped environment.
- **Version 1.1.2**
    - Resolved an export issue with Campaigns without a start or end date.
- **Version 1.1.1**
    - Fixed an object reference issue for Reports.
    - Added support for Filename indicators.
- **Version 1.1.0**
    - Updated the operation to ThreatQuotient Engineering standards. The support tier has been updated from Not Supported to ThreatQ Supported.
    - The **Convert Events to Incident Objects** configuration parameter has been updated to **Convert Events to Which Object**. You can now select the type of STIX object to convert events to or to ignore the events. See the Configuration chapter for more details.
    - Added a new parameter to the Create Bundle Action: TLP selection. See the Actions chapter for more details.
    - Added support for the Intrusion Set system object.
    - Fixed issues where
        - The Hide Original Source action configuration setting was not followed.
        - Exploit Target system objects were not correctly supported.
        - The Create Sighting action did not correctly support SHA-384, SHA-512, ASN, File Path, Mutex, and Registry Key types.
        - An error would occasionally occur for indicators regarding the last_seen and first_seen entries.
- **Version 1.0.0**
    - Initial release