ThreatQuotient

MITRE ATT&CK ICS CDF Guide

Version 1.0.0

January 29, 2022

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

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.

Versioning

- Current integration version `1.0.0`
- Compatible with ThreatQ versions >= `4.35.0`

Introduction

The MITRE ATT&CK ICS CDF for ThreatQuotient enables the automatic ingestion of Common Weakness Enumerations, distributed by MITRE.

The MITRE ATT&CK ICS CDF integration for ThreatQ provides the following feed:

- **MITRE ATT&CK ICS** - brings Attack Patterns, Course of Actions, Intrusion Sets and Malware distributed by MITRE.

The integration ingests the following objects:

- Attack Pattern
  - Attack Pattern Attributes
- Courses of Action
  - Courses of Action Attributes
- Malware
  - Malware Attributes
- Intrusion Set
  - Intrusion Set Attributes

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 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.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

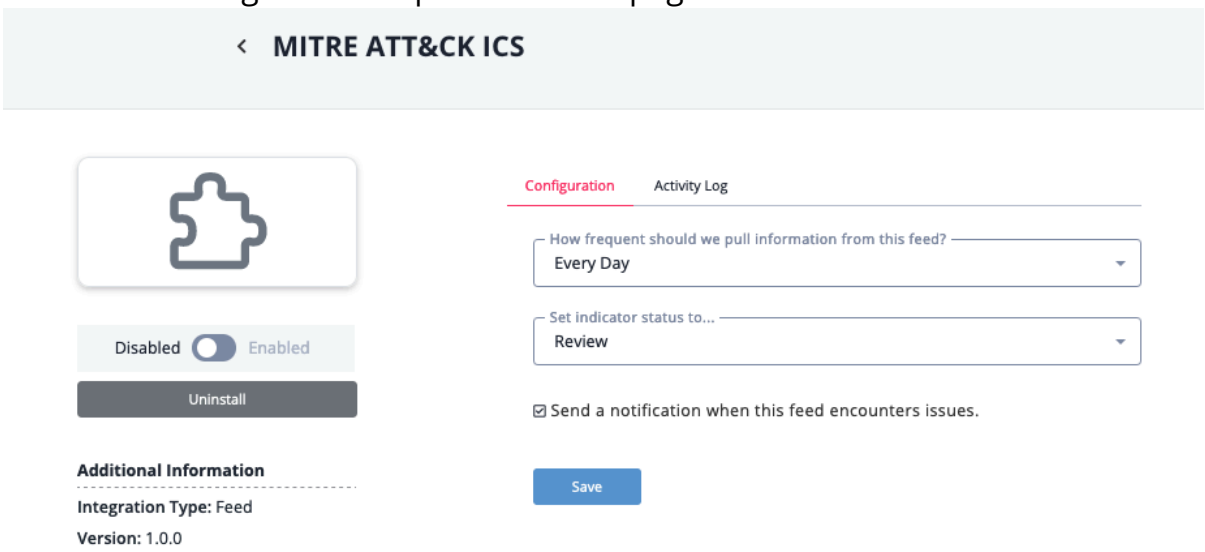
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** 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 to open its details page.



4. Review the 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

MITRE ATT&CK ICS

The MITRE ATT&CK ICS feed brings Attack Patterns, Course of Actions, Intrusion Sets and Malware distributed by MITRE.

`https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json`

Sample Response:


```
{
    "objects": [
        {
            "type": "attack-pattern",
            "name": "Block Command Message",
            "description": "Adversaries may block a command message from reaching its intended target to prevent
command execution.",
            "kill_chain_phases": [
                {
                    "kill_chain_name": "mitre-ics-attack",
                    "phase_name": "execution-ics"
                },
                {
                    "kill_chain_name": "mitre-ics-attack",
                    "phase_name": "evasion-ics"
                }
            ],
            "x_mitre_platforms": [
                "Field Controller/RTU/PLC/IED",
                "Device Configuration/Parameters"
            ],
            "external_references": [
                {
                    "url": "https://collaborate.mitre.org/attackics/index.php/Technique/T0803",
                    "source_name": "mitre-ics-attack",
                    "external_id": "T0803"
                }
            ],
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
            "created": "2020-05-21T17:43:26.506Z",
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "x_mitre_data_sources": [
                "Network Traffic: Network Traffic Flow",
                "Network Traffic: Network Connection Creation",
                "Operational Databases: Process/Event Alarm"
            ],
            "x_mitre_contributors": [
                "Dragos Threat Intelligence"
            ],
            "modified": "2021-10-08T13:04:01.612Z",
```

```
            "id": "attack-pattern--008b8f56-6107-48be-aa9f-746f927dbb61",
            "x_mitre_deprecated": "true"
        },
        {
            "id": "course-of-action--059ba11e-e3dc-49aa-84ca-88197f40d4ea",
            "type": "course-of-action",
            "labels": [
                "NIST SP 800-53 Rev. 4 - SI-3",
                "IEC 62443-3-3:2013 - SR 5.4",
                "IEC 62443-4-2:2019 - CR 5.4"
            ],
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
            "created": "2019-06-11T17:06:56.230Z",
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "external_references": [
                {
                    "source_name": "mitre-ics-attack",
                    "url": "https://collaborate.mitre.org/attackics/index.php/Mitigation/M0948",
                    "external_id": "M0948"
                }
            ],
            "description": "Restrict execution of code to a virtual environment on or in transit to an endpoint
system.",
            "x_mitre_version": "1.0",
            "modified": "2021-04-10T14:17:03.851Z",
            "name": "Application Isolation and Sandboxing"
        },
        {
            "aliases": [
                "ALLANITE",
                "Palmetto Fusion"
            ],
            "type": "intrusion-set",
            "name": "ALLANITE",
            "description": "[ALLANITE](https://collaborate.mitre.org/attackics/index.php/Group/G0009) is a suspected
Russian cyber espionage group.",
            "external_references": [
                {
                    "external_id": "G1000",
                    "source_name": "mitre-ics-attack",
                    "url": "https://collaborate.mitre.org/attackics/index.php/Group/G0009"
                },
                {
                    "description": "(Citation: Dragos ALLANITE)",
                    "source_name": "ALLANITE"
                },
                {
                    "source_name": "Dragos ALLANITE",
                    "description": "Dragon. (n.d.). Allanite. Retrieved October 27, 2019",
                    "url": "https://www.dragos.com/threat/allanite/"
                }
            ],
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "created": "2017-05-31T21:31:57.307Z",
            "id": "intrusion-set--190242d7-73fc-4738-af68-20162f7a5aae",
            "modified": "2020-01-05T23:05:19.419Z",
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
```

```
            "x_mitre_contributors": [
                "Edward Millington"
            ],
            "x_mitre_version": "1.0"
        },
        {
            "modified": "2021-10-13T21:54:51.532Z",
            "x_mitre_version": "1.0",
            "id": "malware--00e7d565-9883-4ee5-b642-8fd17fd6a3f5",
            "type": "malware",
            "description": "[EKANS](https://attack.mitre.org/software/S0605) is ransomware variant that first
appeared in mid-December 2019.",
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "labels": [
                "malware"
            ],
            "external_references": [
                {
                    "external_id": "S0605",
                    "url": "https://attack.mitre.org/software/S0605",
                    "source_name": "mitre-attack"
                },
                {
                    "source_name": "EKANS",
                    "description": "(Citation: Dragos EKANS)(Citation: Palo Alto Unit 42 EKANS)(Citation: FireEye
Ransomware Feb 2020)"
                }
            ],
            "name": "EKANS",
            "object_marking_refs": [
                "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
            ],
            "x_mitre_aliases": [
                "EKANS",
                "SNAKEHOSE"
            ],
            "x_mitre_platforms": [
                "Windows"
            ],
            "created": "2021-02-12T20:07:42.883Z",
            "x_mitre_contributors": [
                "Edward Millington"
            ]
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].external_references[].external_id - .objects[].name	Attack Pattern.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].external_references[].source_name is `mitre-ics-attack`. .objects[].external_references[].external_id is the value for .objects[].external_references[].source_name = `mitre-ics-attack`
.objects[].description	Attack Pattern.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	If .objects[].external_references[].source_name is `mitre-ics-attack`
.objects[].kill_chain_phases[].phase_name	Attack Pattern.Attribute	Kill Chain Phase	.objects[].created	inhibit-response-function	If .objects[].external_references[].source_name is `mitre-ics-attack`
.objects[].x_mitre_platforms[]	Attack Pattern.Attribute	MITRE Platform	.objects[].created	Field Controller/ RTU/PLC/IED	If .objects[].external_references[].source_name is `mitre-ics-attack`
.objects[].x_mitre_data_sources[]	Attack Pattern.Attribute	Data Source	.objects[].created	Network Traffic: Network Traffic Flow	If .objects[].external_references[].source_name is `mitre-ics-attack`
.objects[].x_mitre_deprecated	Attack Pattern.Attribute	Deprecated	.objects[].created	true	If .objects[].external_references[].source_name is `mitre-ics-attack`
.objects[].x_mitre_contributors	Attack Pattern.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	If .objects[].external_references[].source_name is `mitre-ics-attack`
.objects[].external_references[].external_id - .objects[].name	Course Of Action.Value	N/A	.objects[].created	M0801 - Application Isolation and Sandboxing	If .objects[].external_references[].source_name is `course-of-action`. .objects[].external_references[].external_id is the value for .objects[].external_references[].source_name = `mitre-ics-attack`
.objects[].description	Course Of Action.Description	N/A	.objects[].created	Restrict execution of code to a virtual environment	If .objects[].external_references[].source_name is `course-of-action`
.objects[].labels	Course Of Action.Attribute	Label	.objects[].created	NIST SP 800-53 Rev. 4 - SI-3	If .objects[].external_references[].source_name is `course-of-action`
.objects[].external_references[].external_id - .objects[].name	Intrusion Set.Value	N/A	.objects[].created	G1000 - ALLANITE	If .objects[].external_references[].source_name is `intrusion-set`. .objects[].external_references[].external_id is the value for .objects[].external_references[].source_name = `mitre-ics-attack`
.objects[].description	Intrusion Set.Description	N/A	.objects[].created	ALLANITE is a suspected	If .objects[].external_references[].source_name is `intrusion-set`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].aliases	Intrusion Set.Attribute	Alias	.objects[].created	Palmetto Fusion	If .objects[].external_references[].source_name is `intrusion-set`
.objects[].x_mitre_contributors	Intrusion Set.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	If .objects[].external_references[].source_name is `intrusion-set`
.objects[].external_references[]. external_id - .objects[].name	Malware.Value	N/A	.objects[].created	S0605 - EKANS	If .objects[].external_references[]. source_name is `malware`. .objects[].external_ references[].external_id is the value for .objects[].external_references[]. source_name = `mitre-ics-attack`
.objects[].description	Malware.Description	N/A	.objects[].created	EKANS is ransomware..	If .objects[].external_references[].source_name is `malware`
.objects[].x_mitre_aliases	Malware.Attribute	Alias	.objects[].created	SNAKEHOSE	If .objects[].external_references[].source_name is `malware`
.objects[].x_mitre_platforms[]	Malware.Attribute	MITRE Platform	.objects[].created	Windows	If .objects[].external_references[].source_name is `malware`
.objects[].x_mitre_contributors	Malware.Attribute	Contributor	.objects[].created	Edward Millington	If .objects[].external_references[].source_name is `malware`

Average Feed Run

METRIC	RESULT
Run Time	1 minute
Attack Pattern	90
Attack Pattern Attributes	559
Course Of Action	50
Course Of Action Attributes	111
Malware	50
Malware Attributes	111
Intrusion Set	2
Intrusion Set Attributes	4

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.

Change Log

- **Version 1.0.0**
  - Initial release