ThreatQuotient

MITRE ATT&CK CDF

Version 1.1.0

December 17, 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

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	1.1.0
Compatible with ThreatQ Versions	>= 4.19.0
Support Tier	ThreatQ Supported

Introduction

The MITRE ATT&CK CDF integration provides feeds to ingest content from the MITRE Enterprise, Mobile, and ICS ATT&CK collections.

The CDF provides the following feeds:

- **MITRE Enterprise ATT&CK** - retrieves the content of the `Enterprise ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.
- **MITRE Mobile ATT&CK** - retrieves the content of the `Mobile ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.
- **MITRE ICS ATT&CK** - retrieves the content of the ICS ATT&CK collection. It retrieves a list of adversaries, intrusion set, campaigns, course of actions, malware objects, attack patterns and tools, along with their attributes.

The integration ingests the following system objects:

- Adversaries / Intrusion Sets
  - Adversary /Intrusion Set Attributes
- Attack Patterns
  - Attack Pattern Attributes
- Campaigns
- Course of Action
  - Course of Action Attributes
- Malware
  - Malware Attributes
- Tools
  - Tool 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
6. Select the individual feeds to install, when prompted, and then 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(s).

Configuration

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

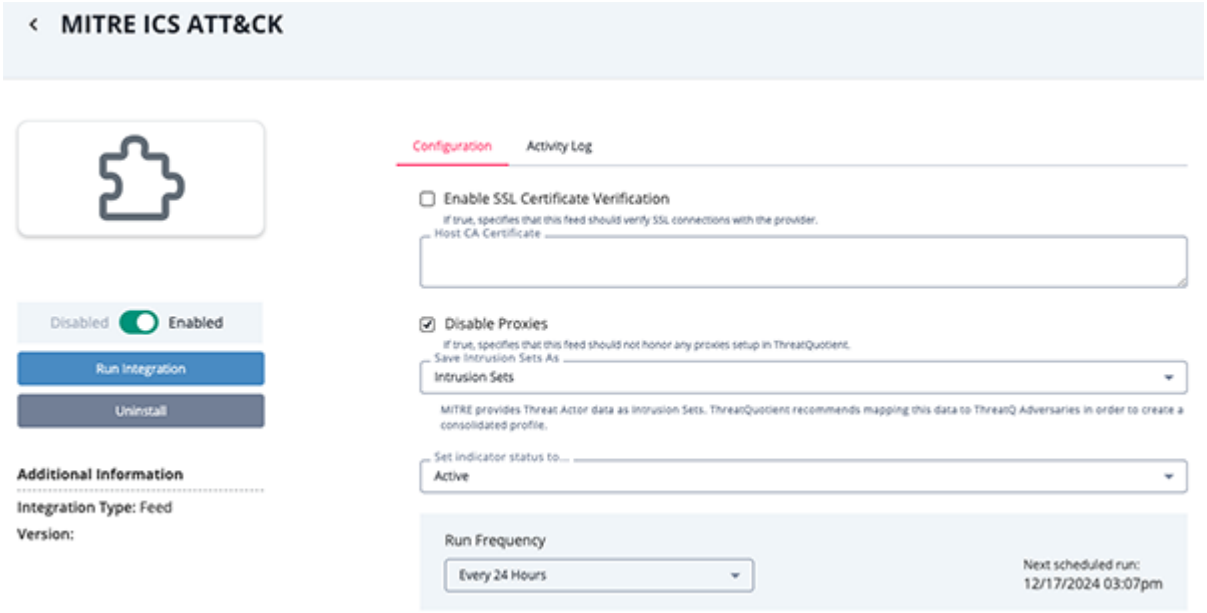
To configure the integration:

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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Host CA	Enter your base64 PEM encoded CA Certificate bundle to verify against the provider's SSL. You can leave this field blank if you did not enable the Verify SSL option listed above.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Save Intrusion Set as	MITRE provides Threat Actor data as Intrusion Sets. Select how you will save the information. Options include: ◦ Adversaries (default) ◦ Intrusion Sets



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

All feeds access the same endpoint, `https://attack-taxii.mitre.org/taxii2/`, each requesting the content of a specific collection.

MITRE Enterprise ATT&CK

The MITRE Enterprise ATT&CK feed retrieves the content of the `Enterprise ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.

Sample Response:


```
{
  "objects": [
    {
      "created": "2021-10-08T14:06:28.212Z",
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "description": "Adversaries may downgrade or use a version of system
features that may be outdated, vulnerable, and/or does not support updated
security controls..",
      "external_references": [
        {
          "external_id": "T1562.010",
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/techniques/T1562/010"
        },
        {
          "description": "Falcon Complete Team. (2021, May 11). Response When
Minutes Matter: Rising Up Against Ransomware. Retrieved October 8, 2021.",
          "source_name": "CrowdStrike BGH Ransomware 2021",
          "url": "https://www.crowdstrike.com/blog/how-falcon-complete-stopped-
a-big-game-hunting-ransomware-attack/"
        }
      ],
      "id": "attack-pattern--824add00-99a1-4b15-9a2d-6c5683b7b497",
      "kill_chain_phases": [
        {
          "kill_chain_name": "mitre-attack",
          "phase_name": "defense-evasion"
        }
      ],
      "modified": "2021-10-15T00:48:06.723Z",
      "name": "Downgrade Attack",
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
```

```
      "type": "attack-pattern",
      "x_mitre_data_sources": [
        "Command: Command Execution",
        "Process: Process Creation"
      ],
      "x_mitre_detection": "Monitor for commands or other activity that may be
indicative of attempts to abuse older or deprecated technologies (ex:
<code>powershell -v 2</code>). ",
      "x_mitre_is_subtechnique": true,
      "x_mitre_permissions_required": [
        "User"
      ],
      "x_mitre_platforms": [
        "Windows"
      ],
      "x_mitre_version": "1.0",
      "x_mitre_system_requirements": [
        "Some folders may require Administrator, SYSTEM or specific user
depending on permission levels and access controls"
      ],
      "x_mitre_is_subtechnique:" true,
      "x_mitre_network_requirements": true
    }
  ]
}
```

ThreatQuotient 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 / Course Of Action / Malware.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].type is `attack-pattern`
.objects[].name	Adversary / Intrusion set / Malware.Value	N/A	.objects[].created	APT17	If .objects[].type is `intrusion-set`
.objects[].description	All objects.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	N/A
.objects[].external_references[]. external_id	Attack Pattern.Attribute	Technique ID	.objects[].created	T1546.009	N/A
.objects[].external_references[]. external_id	Related Adversary/ Intrusion Set.Attribute	Group ID	.objects[].created	G0034	If .objects[].external_references[]. source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[]. external_id	Course Of Action.Attribute	Mitigation ID	.objects[].created	M1014	If .objects[].external_references[]. source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[]. external_id	Tool.Attribute	Tool ID	.objects[].created	S0298	If .objects[].external_references[]. source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[]. external_id	Malware.Attribute	Malware ID	.objects[].created	S0321	If .objects[].external_references[]. source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[]. description	All objects.Attribute	External Reference	.objects[].created	Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) ..	N/A
.objects[].external_references[]. url	All objects.Attribute	External Reference	.objects[].created	`https://attack.mitre.org/mitigations/M1009`	N/A
.objects[].object_marking_refs	All objects.Attribute	Statement Marking	.objects[].created	marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168	If .objects[].external_references[]. source_name is `marking-definition`. Used to filter in to obtain the marking definition (`Copyright 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.`
.objects[].x_mitre_contributors[]	All objects.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	N/A
.objects[].modified	All objects.Attribute	Modified At	.objects[].created	2020-10-26T13:42:49.342Z	N/A
.objects[].x_mitre_deprecated	All objects.Attribute	Deprecated	.objects[].created	true	N/A
.objects[].kill_chain_phases[]. phase_name	Attack Pattern.Attribute	Tactic	.objects[].created	Privilege Escalation	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].x_mitre_difficulty_for_adversary	Attack Pattern.Attribute	Effective Permissions	.objects[].created	Administrator	N/A
.objects[].x_mitre_detection	Attack Pattern.Attribute	Detection	.objects[].created	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process.	N/A
.objects[].x_mitre_data_sources[]	Attack Pattern.Attribute	Data Source	.objects[].created	Command: Command Execution	N/A
.objects[].x_mitre_permissions_required[]	Attack Pattern.Attribute	Permissions Required	.objects[].created	System	N/A
.objects[].x_mitre_system_requirements	Attack Pattern.Attribute	System Requirements	.objects[].created	Some Folders May Require Administrator, System Or Specific User Depending On Permission Levels And Access Controls	N/A
.objects[].x_mitre_defense_bypassed	Attack Pattern.Attribute	Defense Bypassed	.objects[].created	Application Control	N/A
.objects[].x_mitre_effective_permissions[]	Attack Pattern.Attribute	Effective Permissions	.objects[].created	Administrator	N/A
.objects[].x_mitre_network_requirements	Attack Pattern.Attribute	Network Requirements	.objects[].created	true	N/A
.objects[].x_mitre_remote_support	Attack Pattern.Attribute	Remote Support	.objects[].created	true	N/A
.objects[].x_mitre_platforms[]	Attack Pattern / Tool / Malware.Attribute	Platform	.objects[].created	Android	N/A
.objects[].revoked	Attack Pattern / Intrusion set / Malware.Attribute	Revoked	.objects[].created	true	N/A
.objects[].aliases[]	Related Adversary/ Intrusion Set.Value	Alias	.objects[].created	Palmetto Fusion	N/A
.objects[].labels[]	Tool / Malware.Attribute	Label	.objects[].created	tool	N/A

MITRE Mobile ATT&CK

This feed retrieves the content of the `Mobile ATT&CK` collection. It retrieves a list of adversaries, intrusion set, course of actions, malware objects, attack partners and tools, along with their attributes.

Sample Response:


```
{
  "objects": [
    {
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "x_mitre_version": "1.1",
      "external_references": [
        {
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/groups/G0112",
          "external_id": "G0112"
        },
        {
          "source_name": "Bahamut",
          "description": "(Citation: SANS Windshift August 2018)"
        },
        {
          "url": "https://www.sans.org/cyber-security-summit/archives/file/
summit-archive-1554718868.pdf",
          "source_name": "SANS Windshift August 2018",
          "description": "Karim, T. (2018, August). TRAILS OF WINDSHIFT.
Retrieved June 25, 2020."
        }
      ],
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "created": "2020-06-25T17:16:39.168Z",
      "id": "intrusion-set--afec6dc3-a18e-4b62-b1a4-5510e1a498d1",
      "aliases": ["Windshift", "Bahamut"],
      "modified": "2021-04-26T14:37:33.234Z",
      "type": "intrusion-set",
      "name": "Windshift",
      "description": "[Windshift](https://attack.mitre.org/groups/G0112) is a
threat group that has been active since at least 2017..."
    }
  ]
}
```

ThreatQuotient 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 / Course Of Action / Malware.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].type is `attack-pattern`
.objects[].name	Adversary / Intrusion set / Malware.Value	N/A	.objects[].created	APT17	If .objects[].type is `intrusion-set`
.objects[].description	All objects.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	N/A
.objects[].external_references[].external_id	Course Of Action.Attribute	Mitigation ID	.objects[].created	M1014	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Tool.Attribute	Tool ID	.objects[].created	S0298	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Malware.Attribute	Malware ID	.objects[].created	S0321	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Related Adversary/ Intrusion Set.Attribute	Group ID	.objects[].created	G0034	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].description	All objects.Attribute	External Reference	.objects[].created	Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) ..	N/A
.objects[].external_references[].url	All objects.Attribute	External Reference	.objects[].created	`https://attack.mitre.org/mitigations/M1009`	N/A
.objects[].modified	All objects.Attribute	Modified At	.objects[].created	2020-10-26T13:42:49.342Z	N/A
.objects[].object_marking_refs	All objects.Attribute	Statement Marking	.objects[].created	marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168	If .objects[].external_references[].source_name is `marking-definition`. Used to filter in to obtain the marking definition (`Copyright 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.`
.objects[].x_mitre_deprecated	All objects.Attribute	Deprecated	.objects[].created	true	N/A
.objects[].x_mitre_contributors[]	All objects.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	N/A
.objects[].x_mitre_detection	Attack Pattern.Attribute	Detection	.objects[].created	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				normally loaded into a process.	
.objects[].kill_chain_phases[].phase_name	Attack Pattern.Attribute	Tactic	.objects[].created	organizational-information-gathering	N/A
.objects[].external_references[].external_id	Attack Pattern.Attribute	Technique ID	.objects[].created	T1281	N/A
.objects[].x_mitre_platforms[]	Attack Pattern / Tool / Malware.Attribute	Platform	.objects[].created	Android	N/A
.objects[].x_mitre_tactic_type	Attack Pattern.Attribute	Tactic Type	.objects[].created	Post-Adversary Device Access	N/A
.objects[].revoked	Attack Pattern.Attribute	Revoked	.objects[].created	true	N/A
.objects[].aliases[]	Related Adversary/ Intrusion Set.Value	Alias	.objects[].created	Palmetto Fusion	N/A
.objects[].labels[]	Tool / Malware.Attribute	Label	.objects[].created	tool	N/A

MITRE ICS ATT&CK

The MITRE ICS ATT&CK feed retrieves the content of the ICS ATT&CK collection. It retrieves a list of adversaries, intrusion set, campaigns, course of actions, malware objects, attack patterns and tools, along with their attributes.

Sample Response:


```
{
  "objects": [
    {
      "modified": "2023-10-13T17:57:06.171Z",
      "name": "Loss of Safety",
      "description": "Adversaries may compromise safety system functions
designed to maintain safe operation of a process when unacceptable or dangerous
conditions occur. Safety systems are often composed of the same elements as
control systems but have the sole purpose of ensuring the process fails in a
predetermined safe manner. \n\nMany unsafe conditions in process control happen
too quickly for a human operator to react to. Speed is critical in correcting
these conditions to limit serious impacts such as Loss of Control and Property
Damage. \n\nAdversaries may target and disable safety system functions as a
prerequisite to subsequent attack execution or to allow for future unsafe
conditionals to go unchecked. Detection of a Loss of Safety by operators can
result in the shutdown of a process due to strict policies regarding safety
systems. This can cause a Loss of Productivity and Revenue and may meet the
technical goals of adversaries seeking to cause process disruptions.",
      "kill_chain_phases": [
        {
          "kill_chain_name": "mitre-ics-attack",
          "phase_name": "impact"
        }
      ],
      "x_mitre_attack_spec_version": "2.1.0",
      "x_mitre_deprecated": false,
      "x_mitre_detection": "",
      "x_mitre_domains": ["ics-attack"],
      "x_mitre_is_subtechnique": false,
      "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-
d1b8b55e40b5",
      "x_mitre_platforms": ["None"],
      "x_mitre_version": "1.0",
      "type": "attack-pattern",
      "id": "attack-pattern--5fa00fdd-4a55-4191-94a0-564181d7fec2",
      "created": "2020-05-21T17:43:26.506Z",
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "revoked": false,
      "external_references": [
        {
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/techniques/T0880",
```

```
          "external_id": "T0880"
        }
      ],
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ]
    }
  ]
}
```

ThreatQuotient 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 / Course Of Action / Malware.Value	N/A	.objects[].created	T0803 - Block Command Message	If .objects[].type is `attack-pattern`
.objects[].name	Adversary / Intrusion set / Malware.Value	N/A	.objects[].created	APT17	If .objects[].type is `intrusion-set`
.objects[].description	All objects.Description	N/A	.objects[].created	Adversaries may block a command message from reaching..	N/A
.objects[].external_references[].external_id	Attack Pattern.Attribute	Technique ID	.objects[].created	T1546.009	N/A
.objects[].external_references[].external_id	Related Adversary/ Intrusion Set.Attribute	Group ID	.objects[].created	G0034	If .objects[].external_references[].source_name is `mitre-ics-attack` or `mitre-attack`
.objects[].external_references[].external_id	Course Of Action.Attribute	Mitigation ID	.objects[].created	M1014	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Tool.Attribute	Tool ID	.objects[].created	S0298	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].external_id	Malware.Attribute	Malware ID	.objects[].created	S0321	If .objects[].external_references[].source_name is `mitre-mobile-attack` or `mitre-attack`
.objects[].external_references[].description	All objects.Attribute	External Reference	.objects[].created	Gregory Scasny. (2015, September 14). Understanding Open Source Intelligence (OSINT) ..	N/A
.objects[].external_references[].url	All objects.Attribute	External Reference	.objects[].created	https://attack.mitre.org/mitigations/M1009	N/A
.objects[].object_marking_refs	All objects.Attribute	Statement Marking	.objects[].created	marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168	If .objects[].external_references[].source_name is `marking-definition`. Used to filter in to obtain the marking definition (`Copyright 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.`
.objects[].x_mitre_contributors[]	All objects.Attribute	Contributor	.objects[].created	Dragos Threat Intelligence	N/A
.objects[].modified	All objects.Attribute	Modified At	.objects[].created	2020-10-26T13:42:49.342Z	N/A
.objects[].x_mitre_deprecated	All objects.Attribute	Deprecated	.objects[].created	true	N/A
.objects[].kill_chain_phases[].phase_name	Attack Pattern.Attribute	Tactic	.objects[].created	Privilege Escalation	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.objects[].x_mitre_difficulty_for_adversary	Attack Pattern.Attribute	Effective Permissions	.objects[].created	Administrator	N/A
.objects[].x_mitre_detection	Attack Pattern.Attribute	Detection	.objects[].created	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process.	N/A
.objects[].x_mitre_data_sources[]	Attack Pattern.Attribute	Data Source	.objects[].created	Command: Command Execution	N/A
.objects[].x_mitre_permissions_required[]	Attack Pattern.Attribute	Permissions Required	.objects[].created	System	N/A
.objects[].x_mitre_system_requirements	Attack Pattern.Attribute	System Requirements	.objects[].created	Some Folders May Require Administrator, System Or Specific User Depending On Permission Levels And Access Controls	N/A
.objects[].x_mitre_defense_bypassed	Attack Pattern.Attribute	Defense Bypassed	.objects[].created	Application Control	N/A
.objects[].x_mitre_effective_permissions[]	Attack Pattern.Attribute	Effective Permissions	.objects[].created	Administrator	N/A
.objects[].x_mitre_network_requirements	Attack Pattern.Attribute	Network Requirements	.objects[].created	true	N/A
.objects[].x_mitre_remote_support	Attack Pattern.Attribute	Remote Support	.objects[].created	true	N/A
.objects[].x_mitre_platforms[]	Attack Pattern / Tool / Malware.Attribute	Platform	.objects[].created	Android	N/A
.objects[].revoked	Attack Pattern / Intrusion set / Malware.Attribute	Revoked	.objects[].created	true	N/A
.objects[].aliases[]	Related Adversary/ Intrusion Set.Value	Alias	.objects[].created	Palmetto Fusion	N/A
.objects[].labels[]	Tool / Malware.Attribute	Label	.objects[].created	tool	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.

MITRE Enterprise ATT&CK

METRIC	RESULT
Run Time	10 minutes
Adversaries / Intrusion Set	344
Adversaries / Intrusion Set Attributes	5,106
Attack Pattern	707
Attack Pattern Attributes	11,139
Campaigns	13
Campaign Attributes	56
Course Of Action	267
Course Of Action Attributes	1,635
Malware	474
Malware Attributes	4,155
Tool	72

METRIC	RESULT
Tool Attributes	603

MITRE Mobile ATT&CK

METRIC	RESULT
Run Time	10 minutes
Adversaries / Intrusion Set	23
Adversaries / Intrusion Set Attributes	673
Attack Pattern	110
Attack Pattern Attributes	1,144
Campaigns	13
Campaign Attributes	56
Course Of Action	13
Course Of Action Attributes	55
Malware	92
Malware Attributes	731
Tool	2
Tool Attributes	18

MITRE ICS ATT&CK

METRIC	RESULT
Run Time	10 minutes
Adversaries / Intrusion Set	82
Adversaries / Intrusion Set Attributes	1808
Attack Pattern	95
Attack Pattern Attributes	1078
Campaigns	7
Campaign Attributes	36
Course Of Action	52
Course Of Action Attributes	347
Malware	23
Malware Attributes	286

Change Log

- **Version 1.1.0**
  - Updated the integration to use MITRE's TAXII v2.1 server.
  - Removed the **MITRE PRE-ATT&CK** feed as it has been deprecated by the provider.
  - Added a new feed: **MITRE ICS ATT&CK**.
  - Added support for Campaign objects.
- **Version 1.0.0**
  - Initial release