ThreatQuotient

McAfee ATD Connector Guide

Version 1.0.0

September 28, 2021

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`
- Supported on ThreatQ versions >= `4.41.0`

Introduction

The McAfee ATD Connector uses the McAfee DXL to ingest information about malware analyses that are performed and utilizes the McAfee ATD REST API to fetch ATD PDF.

The fetched ATD PDF reports will be linked to the main indicator.

The McAfee ATD Connector will only ingest data after being initiated by the user via command line. The connector will continue to ingest data until manually terminated by the user. See the Usage section of this guide for command details.

Installation

The connector can be installed from the ThreatQuotient repository with YUM credentials or offline via a .whl file.

> **Upgrading Users** - Review the Change Log for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. Failure to delete the previous configuration file will result in the connector failing.

1. Install the connector using one of the following methods:

   ThreatQ Repository

   a. Run the following command:

   ```
   <> pip install tq_conn_mcafee_atd
   ```

   Offline via .whl file

   To install this connector from a wheel file, the wheel file (.whl) will need to be copied via SCP into your ThreatQ instance.

   a. Download the connector whl file with its dependencies:

   ```
   <> mkdir /tmp/tq_conn_mcafee_atd

      pip download tq_conn_mcafee_atd -d

      /tmp/tq_conn_mcafee_atd/
   ```

   b. Archive the folder with the .whl files:

   ```
   <> tar -czvf tq_conn_mcafee_atd.tgz /tmp/tq_conn_mcafee_atd/
   ```

   c. Transfer all the whl files, the connector and all the dependencies, to the ThreatQ instance.

   d. Open the archive on ThreatQ:

   ```
   <> tar -xvf tq_conn_mcafee_atd.tgz
   ```

   e. Install the connector on the ThreatQ instance.

> The example assumes that all the whl files are copied to `/tmp/conn` on the ThreatQ instance.

```
<> pip install /tmp/conn/tq_conn_mcafee_atd-<version>-<python
   version>-none-any.whl --no-index --find-links /tmp/conn/
```

> A driver called `tq-conn-mcafee-atd` will be installed. After installing with `pip` or `setup.py`, a script stub will appear in `/usr/bin/mcafee_atd`.

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. Use the commands below to create the required directories:

```
<> mkdir -p /etc/tq_labs/
   mkdir -p /var/log/tq_labs
```

3. Perform an initial run using the following command:

```
<> tq-conn-mcafee-atd -v 3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

4. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
Email Address	This is the User in the ThreatQ System for integrations.
Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

Example Output

```
tq-conn-mcafee-atd v 3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
ThreatQ Host: <ThreatQ Host IP or Hostname>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

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

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 connector:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the *Category* dropdown (optional).

   > If you are installing the connector for the first time, it will be located under the **Disabled** tab.

3. Click on the connector to open its details page.
4. Enter the following parameters:

PARAMETER	DESCRIPTION
ePO Hostname	The ePO instance hostname or IP address.
ePO DXL Registration Port	The ePO instance DXL Registration Port, defaulting to `8443`.
ePO Username	The ePO instance Username.
ePO Password	The ePO instance Password.
ATD Hostname	The ATD instance hostname or IP Address.
ATD Username	The ATD instance username.
ATD Password	The ATD instance password.
Verify SSL	Checking this option will have the connector verify SSL connections with the configured ATD server.

PARAMETER	DESCRIPTION
Event Severity Threshold	The minimum severity for which events are processed. The default for this setting is `Low`.

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

> The McAfee ATD Connector will only ingest data after being initiated by the user via command line. The connector will continue to ingest data until manually terminated by the user. See the Usage section of this guide for command details.

ThreatQ Mapping

McAfee ATD Event

JSON response sample:


```
{
    "Summary": {
        "Bait": "Baitexe activated but not infected",
        "Behavior": [],
        "Data": {
            "analysis_seconds": "79",
            "compiled_with": "Not Available",
            "sandbox_analysis": "5"
        },
        "DETversion": "4.6.0.181109",
        "Files": [
            {
                "FileType": "0",
                "Md5": "",
                "Name": "iexplore.exe",
                "Processes": [
                    {
                        "Name": "iexplore.exe",
                        "RelType": "1",
                        "Sha256": ""
                    }
                ],
                "Sha1": "",
                "Sha256": ""
            }
        ],
        "hasDynamicAnalysis": "true",
        "JobId": "243",
        "JSONversion": "1.003",
        "MISversion": "4.6.0.21",
        "Mitre": [
            {
                "Rules": [
                    {
                        "Description": "Read data from a handle opened on previous URL's request",
                        "Severity": "1"
                    },
                    {
                        "Description": "connected to common ports",
                        "Severity": "1"
                    }
                ],
                "Tactics": "Command and Control",
                "Techniques": "Commonly Used Port"
            }
        ],
        "OSversion": "win2k16p0x64_Win2k16",
        "Process": [
```

```
        {
            "Name": "http://subtitleseeker.com",
            "Reason": "loaded by MATD Analyzer",
            "Severity": "1"
        }
    ],
    "Processes": [
        {
            "Name": "http://subtitleseeker.com",
            "Registry Operations": [
                {
                    "Registry Created": [
                        "HKCU/Software/Microsoft/Windows/CurrentVersion/Internet Settings/P3P/History"
                    ]
                }
            ],
            "Run-Time Dlls": [
                {
                    "DLL Loaded": [
                        "api-ms-win-rtcore-ntuser-wmpointer-l1-1-0.dll",
                        "dcomp.dll"
                    ]
                }
            ]
        }
    ],
    "Selectors": [
        {
            "Engine": "Anti-Malware",
            "MalwareName": "---",
            "Severity": "0"
        }
    ],
    "Stats": [
        {
            "Category": "Data spying, Sniffing, Keylogging, Ebanking Fraud ",
            "ID": "6",
            "Severity": "0"
        }
    ],
    "Subject": {
        "FileType": "4096",
        "md5": "BAE2983970C418BFD22903C5AB3ED569",
        "Name": "http://subtitleseeker.com",
        "parent_archive": "Not Available",
        "sha-1": "4C4ECF4FF55B821A468A26442094 39B5A43FA0E5",
        "sha-256": "3336CD42FEFD2089BFFFB3733BDBF22BFB1B707E8F5EFAEBFD865B0E26ACFFE3",
        "size": "25",
        "Timestamp": "2020-11-02 04:53:56",
        "Type": "application/url"
    },
    "SubmitterName": "robert",
    "SubmitterType": "STAND_ALONE",
    "SUMversion": "4.6.0.21",
    "TaskId": "246",
    "URL_Reputation": [
        {
            "category": "Business ",
            "functional": "Business/Services ",
            "port": "80",
```

```
                "reputation": "Clean",
                "risk": "Information ",
                "severity": "0",
                "url": "IECVLIST.MICROSOFT.COM"
            }
        ],
        "Urls": [
            {
                "Category": "Business ",
                "Functional": "Business/Services ",
                "Port": "80",
                "Processes": [
                    {
                        "Name": "iexplore.exe",
                        "RelType": "8",
                        "Sha256": ""
                    }
                ],
                "Reputation": "-3",
                "Risk": "Information ",
                "Severity": "0",
                "Url": "IECVLIST.MICROSOFT.COM"
            }
        ],
        "Verdict": {
            "Description": "Sample is somewhat suspicious: final severity level 2",
            "Severity": "2"
        }
    }
}
```

The mapping table is provided below:

DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.Summary.Subject.Name	Indicator	URL/Filename	'http://subtitleseeker.com'	
.Summary.Data.compiled_with	Indicator Attribute	Complied With	'Not Available'	
.Summary.Data.sandbox_analysis	Indicator Attribute	Sandbox Analysis	'5'	
.Summary.Files[].Name	Related Indicator	Filename	'iexplore.exe	
.Summary.Files[].Md5	Related Indicator	MD5	N/A	
.Summary.Files[].Sha1	Related Indicator	SHA-1	N/A	
.Summary.Files[].Sha256	Related Indicator	SHA-256	N/A	
.Summary.Files[].Processes[].Sha256	Related Indicator	SHA-256	N/A	
.Summary.hasDynamicAnalysis	Indicator Attribute	Has Dynamic Analysis	'true'	
.Summary.Mitre[].Techniques	Rel. Attack Pattern	N/A	'Commonly Used Port'	Linked to a ThreatQ MITRE Attack Pattern
.Summary.OSversion	Indicator Attribute	OS Version	'win2k16p0x64_Win2k16'	
.Summary.Process[].Reason	Indicator Attribute	Reason	'loaded by MATD Analyzer'	
.Summary.Process[].Severity	Indicator Attribute	Severity	'Informational'	Mapped using the severity level mapping table
.Summary.Processes[]."Registry Operations"[]."Registry Created"[]	Related Indicator	Registry Key	'HKCU/Software/Microsoft/ Windows/CurrentVersion/ Internet Settings/P3P/History'	
.Summary.Processes[]."Run-Time Dlls"[]."DLL Loaded"[]	Related Indicator	Filename	'dcomp.dll'	
.Summary.Selectors[].Severity	Indicator Attribute	Engine `.Summary.Selectors[].Engine` Severity	'Engine Anti-Malware Severity': 'Unverified'	Each word of the attribute name has the first character capitalized, attribute value mapped using the severity level mapping table
.Summary.Stats[].Severity	Indicator Attribute	Category `.Summary.Stats[].Category` Severity	'Category Data Spying Severity': 'Unverified'	Each word of the attribute name has the first character capitalized, attribute value mapped using the severity level mapping table
.Summary.Subject.md5	Related Indicator	MD5	'BAE2983970C418BFD22903 C5AB3ED569'	
.Summary.Subject.sha-1	Related Indicator	SHA-1	'4C4ECF4FF55B821A468A264 4209439B5A43FA0E5'	

DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.Summary.Subject.sha-256	Related Indicator	SHA-256	'3336CD42FEFD2089BFFFB3733BDBF22BFB1B707E8F5EFAEBFD865B0E26ACFFE3'	
.Summary.Urls[]	Related Indicator	URL	'IECVLIST.MICROSOFT.COM'	Review Status
.Summary.URL_Reputation[]	Related Indicator	URL	'IECVLIST.MICROSOFT.COM'	Review Status
.Summary.Verdict.Severity	Indicator Attribute	Threat Level	'Low'	Mapped using the severity level mapping table

The fetched ATD PDF report will be also linked to the main indicator.

Severity Level Mapping

MCAFEE ATD SEVERITY LEVEL	THREATQ ATTRIBUTE VALUE
-2	Failed
-1	Clean
0	Unverified
1	Informational
2	Low
3	Medium
4	High
5	Very High

Usage

The connector shouldn't be executed via a cron job since it acts like a daemon, continuously running until the execution is terminated by the user.

1. Run the connector using the following command:

```
<> tq-conn-mcafee-atd -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/ -rp
```

Command Line Arguments

ARGUMENT	DESCRIPTION
-v (optional)	Sets the log verbosity (3 means everything).
-c (optional)	The path to the directory where you want to store your config file.
-ll (optional)	The path to the directory where you want to store your logs.
-n, --name (optional)	Name of the connector (Option used in order to allow users to configure multiple McAfee ATD connector instances on the same TQ box)
-rp (optional)	If set, the DXL client is re-provisioned with the current user field values instead of using the previously-provisioned certificates stored on disk.

All location-based options default to the current working directory if they are not provided. Invoke the program with `-h` to find additional options and option descriptions.

Known Issues/Limitations

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns to be related. MITRE ATT&CK attack patterns are ingested from the following feeds:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE PRE-ATT&CK
- MITRE ATT&CK data that already exists in ThreatQ will only be reloaded into this connector at most once a day.

Change Log

- **Version 1.0.0**
  - Revamped connector
- **Version 0.8.1**
  - Initial release