ThreatQuotient

McAfee ATD Operation User Guide

Version 1.2.0

November 01, 2023

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	1.2.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The McAfee ATD operation enriches ThreatQ objects with context obtained from the McAfee ATD API.

The operation provides the following actions:

- Get Analyzer Profiles - retrieves the configured ATD analyzer profiles.
- Hash Value Check - checks if the hash is either blacklisted or whitelisted.
- Submit URL - submits a URL for analysis.
- Submit File - submits a file for analysis.
- Get Report - retrieves the report and enriches the threat object

The operation is compatible with Files and URL Indicator types.

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 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
Host	Your McAfee ATD Instance host.
User Name	Your McAfee ATD username.
Password	Your McAfee ATD password.

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
Get Analyzer Profiles	Retrieves the configured ATD analyzer profiles.	Indicators, Files	URL (Indicators)
Hash Value Check	Checks if the hash is either blacklisted or whitelisted.	Indicators	URL
Submit URL	Submits a URL for analysis.	Indicators	URL
Submit File	Submits a file for analysis.	Files	N/A
Get Report	Retrieves the report and enriches the threat object.	Indicators, Files	URL (Indicators)

Get Analyzer Profiles

The Get Analyzer Profiles action is used to retrieve the available analyzer profiles configured on the ATD instance.

```
GET http://<atd-instance-host>/php/vmprofiles.php
```

Hash Value Check

The Hash Value Check action is used to check if the submitted MD5 hash is either blacklisted or whitelisted.

`POST http://<atd-instance-host>/php/atdHashLookup.php`

Sample Response:

```
{
  "results": {
        "E6201BC847D2C9F11B999741704B3E0A": "w"
    },
    "success": true
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.results.	Indicator Attribute	ATD Indicator Status	Hash value is whitelisted.	Automatically added

Submit URL & Submit File

The Submit URL and Submit File actions

used to submit a URL or File to ATD for analysis.

`POST http://<atd-instance-host>/php/fileupload.php`

Sample Response:


```
{
    "estimatedTime": 0,
    "fileId": "",
    "filesWait": 0,
    "mimeType": "application/url",
    "results": [
        {
            "cache": 0,
            "destIp": null,
            "file": "http://subtitleseeker.com",
            "md5": "BAE2983970C418BFD22903C5AB3ED569",
            "messageId": "",
            "sha1": "",
            "sha256": "",
            "size": "25",
            "srcIp": "",
            "submitType": "1",
            "taskId": 246,
            "url": "http://subtitleseeker.com"
        }
    ],
    "subId": 243,
    "success": true
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
subId	Indicator.Attribute	ATD Submission ID	243	Automatically added
.results[].md5	Indicator.Value	MD5	'BAE2983970C418BFD22903C5AB3ED569'	
.results[].sha1	Indicator.Value	SHA-1	N/A	
.results[].sha256	Indicator.Value	SHA-256	N/A	

Configuration Parameters

The following parameters are available for these actions:

PARAMETER	DESCRIPTION
Analyzer Profile IDs	Comma-separated values representing the analyzer profile IDs to be used for sample analysis. The IDs can be retrieved by running the Get Report action. If left empty, all analyzers are used.
File Priority	Indicates the priority of sample analysis.
Source IP	The IPv4 address of the source system or gateway from where the file is downloaded
Destination IP	The IPv4 address of the target endpoint.
YARA Scanner	Indicates the custom YARA scanner settings that need to be set for the provided `Analyzer Profile IDs`. There are three options to choose from. Choosing either `Enable` or `Disable` will change the custom YARA scanner to be enabled or disabled, respectively. Choosing `Keep Settings` will use the current settings for the YARA scanner. The current YARA scanner status can be retrieved by running the Get Analyzer Profiles action.

Get Report

The Get Report action is used to retrieve the submission report(s) for the submitted threat object.

`GET http://<atd-instance-host>/php/configloader/getremoteshowreport.php`

Sample Response:


```
  "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": "4C4ECF4FF55B821A468A2644209439B5A43FA0E5",
            "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"
        }
    }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.Summary.Data.compiled_with	Indicator.Attribute	Complied With	'Not Available'	
.Summary.Data.sandbox_analysis	Indicator.Attribute	Sandbox Analysis	'5'	
.Summary.Files[].Name	Indicator.Value	Filename	'iexplore.exe	
.Summary.Files[].Md5	Indicator.Value	MD5	N/A	
.Summary.Files[].Sha1	Indicator.Value	SHA1	N/A	
.Summary.Files[].Sha256	Indicator.Value	SHA256	N/A	
.Summary.Files[].Processes[].Sha256	Indicator.Value	SHA256	N/A	
.Summary.hasDynamicAnalysis	Indicator.Attribute	Has Dynamic Analysis	'true'	
.Summary.Mitre[].Techniques	Attack Pattern.Value	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[]	Indicator.Value	Registry Key	'HKCU/Software/Microsoft/Windows/CurrentVersion/Internet Settings/P3P/History'	
.Summary.Processes[].Run-Time Dlls[].DLL Loaded[]	Indicator.Value	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 its first character capitalized. The attribute value is mapped using the severity level mapping table.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.Summary.Stats[].Severity	Indicator.Attribute	Category `.Summary.Stats[].Category` Severity	'Category Data Spying Severity': 'Unverified'	Each word of the attribute name has its first character capitalized. The attribute value is mapped using the severity level mapping table.
.Summary.Subject.md5	Indicator.Value	MD5	'BAE2983970C418BFD 22903C5AB3ED569'	
.Summary.Subject.sha-1	Indicator.Value	SHA1	'4C4ECF4FF55B821A46 8A2644209439B5A4 3FA0E5'	
.Summary.Subject.sha-256	Indicator.Value	SHA256	'3336CD42FEFD2089BFFFB 3733BDBF22BFB1B707E8F 5EFAEBFD865B0E 26ACFFE3'	
.Summary.Urls[]	Indicator.Value	URL	'IECVLIST.MICROSOFT.COM'	Review Status
.Summary.URL_Reputation[]	Indicator.Value	URL	'IECVLIST.MICROSOFT.COM'	Review Status
.Summary.Verdict.Severity	Indicator.Attribute	Threat Level	'Low'	Mapped using the severity level mapping table

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

Change Log

- **Version 1.2.0**
  - Added the ability to submit URL samples with a `Scheme` attribute defined.
- **Version 1.1.0**
  - Add threat severity mapping to severity attributes
  - Normalize attributes between connector and operation
- **Version 1.0.0**
  - Revamped operation
- **Version 0.1.0**
  - Initial release