

# ThreatQuotient



## ThreatQ Action Bundle for Microsoft Azure Sentinel User Guide

Version 1.0.1

March 15, 2024

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147



ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

|  |    |
|--|----|
| Warning and Disclaimer .....                     | 3  |
| Support .....                                    | 4  |
| Integration Details.....                         | 5  |
| Introduction .....                               | 6  |
| Prerequisites .....                              | 7  |
| Installation.....                                | 8  |
| Configuration .....                              | 9  |
| Actions .....                                    | 12 |
| Microsoft Azure Sentinel Enrich Indicators ..... | 13 |
| Microsoft Azure Sentinel Add Tag .....           | 16 |
| Microsoft Azure Sentinel Export Collection ..... | 18 |
| Microsoft Azure Sentinel Delete Collection.....  | 19 |
| Enriched Data.....                               | 20 |
| Microsoft Azure Sentinel Enrich Indicators.....  | 20 |
| Microsoft Azure Sentinel Add Tag .....           | 20 |
| Known Issues / Limitations .....                 | 21 |
| Change Log .....                                 | 22 |

# 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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto: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      | 1.0.1             |
| Compatible with ThreatQ Versions | >= 5.12.1         |
| ThreatQ TQO License Required     | Yes               |
| Support Tier                     | ThreatQ Supported |

# Introduction

The ThreatQ Action Bundle for Microsoft Azure Sentinel provides actions that are used to enrich a specific collection and to add or delete them to/from your Microsoft Azure Sentinel instance.

The action yaml installs the following actions:

- **Microsoft Azure Sentinel Enrich Indicators** - queries indicators contained in a threat-library against Microsoft Sentinel and enriches them with the returned data.
- **Microsoft Azure Sentinel Add Tag** - adds user defined tags to indicators contained in a threat-collection both in the Microsoft Sentinel context and in TQ.
- **Microsoft Azure Sentinel Export Collection** - queries indicators contained in a threat-library against Microsoft Sentinel and adds them if not present.
- **Microsoft Azure Sentinel Delete Collection** - queries indicators contained in a threat-library against Microsoft Sentinel and deletes them if present.

The actions are compatible with the following indicator types:

- FQDN
- IP Address
- URL
- SHA-256
- MD5

The actions return the following enrich system objects:

- Indicators
  - Indicator Attributes



This action bundle is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

# Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator objects:
  - FQDN
  - IP Address
  - URL
  - SHA-256
  - MD5

# 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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
  - Drag and drop the zip file into the dialog box
  - Select **Click to Browse** to locate the zip file on your local machine



ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to [configure](#) the action.



# 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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:



The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

| PARAMETER       | DESCRIPTION  |
|-----------------|--|
| Tenant ID       | Your Azure Tenant ID which can be retrieved from the App Registrations page in Azure Active Directory.     |
| Client ID       | Your Azure Client ID that can be retrieved from the App Registrations page in Azure Active Directory.      |
| Client Secret   | Your Azure Client Secret which can be retrieved from the Certificates & Secrets section.                   |
| Subscription ID | Your Azure subscription ID, obtained from the Log Analytics Workspaces.                                    |
| Resource Group  | The name of the resource group within the user's subscription, obtained from the Log Analytics Workspaces. |
| Workspace Name  | The name of the workspace, obtained from the Log Analytics Workspaces.                                     |
| Tags            | Enter a list of tags to be appended (separated by a comma).  |

| PARAMETER               | DESCRIPTION  |
|-------------------------|--|
|                         |  This parameter is only available for the <b>Microsoft Azure Add Tag</b> action.  |
| Default Expiration Days | Enter the number of days the indicators remain valid.<br> This parameter is only available for the <b>Microsoft Azure Export Collection</b> action. |
| Hostname                | Your ThreatQ Hostname.<br> This parameter is only available for the <b>Microsoft Azure Export Collection</b> action.                                |

## < Microsoft Azure Sentinel Export Collection



Uninstall

### Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

### Configuration

Tenant ID

Retrieved from the App Registrations page in Azure Active Directory

Client ID

Retrieved from the App Registrations page in Azure Active Directory

Client Secret

This is obtained from your Azure Active Directory Certificates and Secrets

Subscription ID

This is obtained from the Log Analytics Workspaces

Resource Group

This is obtained from the Log Analytics Workspaces

Workspace Name

Default Expiration Days

30

How many days should these indicators remain valid

Hostname

ThreatQ Hostname

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.

# Actions

The following actions are available:

| FUNCTION   | DESCRIPTION   | OBJECT<br>TYPE | OBJECT SUBTYPE                         |
|--|---|----------------|--|
| Microsoft Azure<br>Sentinel Enrich<br>Indicators | Enrich Indicators with<br>attributes.               | Indicators     | IP Address, URL,<br>FQDN, MD5, SHA-256 |
| Microsoft Azure<br>Sentinel Add Tag              | Add custom tags to the<br>Indicators.               | Indicators     | IP Address, URL,<br>FQDN, MD5, SHA-256 |
| Microsoft Azure<br>Sentinel Export<br>Collection | Add Indicators to<br>Microsoft Azure Sentinel.      | Indicators     | IP Address, URL,<br>FQDN, MD5, SHA-256 |
| Microsoft Azure<br>Sentinel Delete<br>Collection | Delete Indicators from<br>Microsoft Azure Sentinel. | Indicators     | IP Address, URL,<br>FQDN, MD5, SHA-256 |

## Microsoft Azure Sentinel Enrich Indicators

This Microsoft Azure Sentinel Enrich Indicators action enriches the selected collection with attributes, tags and description.

```
POST "https://management.azure.com/subscriptions/{{subscription_id}}/
resourceGroups/{{resource_group}}/providers/Microsoft.OperationalInsights/
workspaces/{{workspace}}/providers/Microsoft.SecurityInsights/
threatIntelligence/main/queryIndicators?api-version=2021-10-01"
```

### Sample Body

Form URL-Encoded

```
{"keywords": "114.33.22.185"}
```

### Sample Response

```
{
  "value": [
    {
      "id": "/subscriptions/f1c10b41-49ff-4791-b366-b3bbb37fca4c/
resourceGroups/group1/providers/Microsoft.OperationalInsights/workspaces/
tqsentinal/providers/Microsoft.SecurityInsights/threatIntelligence/46a89ec4-
edc9-811f-1700-99f8b261ca6a",
      "name": "46a89ec4-edc9-811f-1700-99f8b261ca6a",
      "etag": "\"35007697-0000-0100-0000-6273b4eb0000\"",
      "type": "Microsoft.SecurityInsights/threatIntelligence",
      "kind": "indicator",
      "properties": {
        "confidence": 0,
        "created": "2022-01-25T15:24:50.2947152Z",
        "extensions": {
          "sentinelExtension": {
            "severity": null
          },
          "isg-source-ext": {
            "azureTenantId": "0b5a4827-4085-4ca9-a477-69bfd6ec7b76",
            "networkIPv4": "114.33.22.185",
            "targetProduct": "Azure Sentinel",
            "threatType": "Darknet",
            "id":
"0FAAB80706511F8F98301255D29FA34D1319303EC2A07374B85155E63E5A6CE4",
            "ingestedDateTime": "2022-01-25T15:24:18.259557+00:00",
            "action": "allow",
            "additionalInformation": "https://127.0.0.1/indicators/
6793/details",
            "activityGroupNames": [],
            "confidence": 0,
            "description": "IOC exported from ThreatQ",
            "expirationDateTime": "2022-07-25T15:22:43+00:00",
            "externalId": "6793",
```

```

        "isActive": true,
        "killChain": [],
        "lastReportedDateTime": "2022-01-25T12:54:53+00:00",
        "malwareFamilyNames": [],
        "severity": 5,
        "tags": [],
        "tlpLevel": "unknown"
    },
    },
    "externalId": "indicator--001c5557-1145-5521-9967-eebe843d32ff",
    "externalLastUpdatedTimeUtc": "2022-01-25T15:24:18.259557Z",
    "lastUpdatedTimeUtc": "2022-01-25T15:24:50.2947486Z",
    "source": "SecurityGraph",
    "threatIntelligenceTags": [
        "tg1",
        "Test_tag",
        " Tag_2"
    ],
    "displayName": "Custom Threat Intelligence",
    "description": "IOC exported from ThreatQ",
    "threatTypes": [
        "Darknet"
    ],
    "parsedPattern": [
        {
            "patternTypeKey": "ipv4-addr",
            "patternTypeValues": [
                {
                    "valueType": "ipv4-addr",
                    "value": "114.33.22.185"
                }
            ]
        }
    ],
    "pattern": "[ipv4-addr:value = '114.33.22.185']",
    "patternType": "stix",
    "validFrom": "2022-01-25T15:24:18.259557Z",
    "validUntil": "2022-07-25T15:22:43Z"
}
}
]
}

```

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH                             | THREATQ ENTITY        | THREATQ OBJECT<br>TYPE OR<br>ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES                     | NOTES |
|--|-----------------------|--|----------------|------------------------------|-------|
| .value[].properties.description            | Indicator.Description | N/A  | N/A            | IOC exported<br>from ThreatQ | N/A   |
| .value[].properties.threatIntelligenceTags | Indicator.Tag         | N/A  | N/A            | tg1                          | N/A   |

| FEED DATA PATH   | THREATQ ENTITY      | THREATQ OBJECT<br>TYPE OR<br>ATTRIBUTE KEY | PUBLISHED DATE              | EXAMPLES      | NOTES |
|--|---------------------|--|-----------------------------|---------------|-------|
| .value[].properties.confidence                           | Indicator.Attribute | Confidence                                 | .value[].properties.created | 0             | N/A   |
| .value[].properties.extensions.isg-source-ext.severity   | Indicator.Attribute | Severity                                   | .value[].properties.created | 5             | N/A   |
| .value[].properties.extensions.isg-source-ext.threatType | Indicator.Attribute | Threat Type                                | .value[].properties.created | Darknet       | N/A   |
| .value[].properties.source                               | Indicator.Attribute | Source                                     | .value[].properties.created | SecurityGraph | N/A   |

## Microsoft Azure Sentinel Add Tag

The Microsoft Azure Sentinel Add Tag action will enrich the selected collection with custom tags.

```
POST "https://management.azure.com/subscriptions/{{subscription_id}}/
resourceGroups/{{resource_group}}/providers/Microsoft.OperationalInsights/
workspaces/{{workspace}}/providers/Microsoft.SecurityInsights/
threatIntelligence/main/indicators/{{id}}/appendTags?api-version=2021-10-01"
```

### Sample Body

Form URL-Encoded

```
{"threatIntelligenceTags": "tag1"}
```

### Sample Response

```
{
  "id": "/subscriptions/f1c10b41-49ff-4791-b366-b3bbb37fca4c/resourceGroups/
group1/providers/Microsoft.OperationalInsights/workspaces/tqsentinal/providers/
Microsoft.SecurityInsights/threatIntelligence/
68cb63da-7104-79ea-3e90-0d48e8da87d3",
  "name": "68cb63da-7104-79ea-3e90-0d48e8da87d3",
  "etag": "\"3500e992-0000-0100-0000-6273b2440000\"",
  "type": "Microsoft.SecurityInsights/threatIntelligence",
  "kind": "indicator",
  "properties": {
    "confidence": 0,
    "created": "2022-01-25T15:24:46.0253884Z",
    "extensions": {
      "sentinelExtension": {
        "severity": null
      },
      "isg-source-ext": {
        "azureTenantId": "0b5a4827-4085-4ca9-a477-69bfd6ec7b76",
        "networkIPv4": "82.157.168.58",
        "targetProduct": "Azure Sentinel",
        "threatType": "Darknet",
        "id":
"FD300635CCE291874D9261CF32C969E040BF170383F3498783DCB46044F9D4C4",
        "ingestedDateTime": "2022-01-25T15:23:56.0167939+00:00",
        "action": "allow",
        "additionalInformation": "https://127.0.0.1/indicators/4856/
details",
        "activityGroupNames": [],
        "confidence": 0,
        "description": "IOC exported from ThreatQ",
        "expirationDateTime": "2022-07-25T15:22:43+00:00",
        "externalId": "4856",
        "isActive": true,
        "killChain": [],
        "lastReportedDateTime": "2022-01-25T12:53:37+00:00",
```



```

        "malwareFamilyNames": [],
        "severity": 5,
        "tags": [],
        "tlpLevel": "unknown"
    },
    },
    "externalId": "indicator--ffdafea4-f410-5a4a-bc71-a1f1e2d2b9ab",
    "externalLastUpdatedTimeUtc": "2022-01-25T15:23:56.0167939Z",
    "lastUpdatedTimeUtc": "2022-01-25T15:24:46.0254189Z",
    "source": "SecurityGraph",
    "threatIntelligenceTags": [
        "tag1",
        "tag2"
    ],
    "displayName": "Custom Threat Intelligence",
    "description": "IOC exported from ThreatQ",
    "threatTypes": [
        "Darknet"
    ],
    "parsedPattern": [
        {
            "patternTypeKey": "ipv4-addr",
            "patternTypeValues": [
                {
                    "valueType": "ipv4-addr",
                    "value": "82.157.168.58"
                }
            ]
        }
    ],
    "pattern": "[ipv4-addr:value = '82.157.168.58']",
    "patternType": "stix",
    "validFrom": "2022-01-25T15:23:56.0167939Z",
    "validUntil": "2022-07-25T15:22:43Z"
}
}

```

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH                       | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--------------------------------------|----------------|--------------------------------------|----------------|----------|-------|
| .properties.threatIntelligenceTags[] | Indicator.Tag  | N/A                                  | N/A            | tag1     | N/A   |

## Microsoft Azure Sentinel Export Collection

The Microsoft Azure Sentinel Add Tag action enriches the selected collection with attributes, tags and description.



This action only pushes a collection of Indicators to Microsoft Azure Sentinel, and does not ingest threat data back into the ThreatQ platform.

POST "https://sentinelus.azure-api.net/{{workspace\_id}}/  
threatintelligence:upload-indicators?api-version=2022-07-01"

### Sample Body

Form URL-Encoded

```
{
  "kind": "indicator",
  "properties": {
    "source": "Azure Sentinel",
    "displayName": "Custom Threat Intelligence",
    "description": "IOC exported from ThreatQ",
    "threatTypes": [
      "compromised"
    ],
    "pattern": "[file:hashes.MD5 = 008b81f89405228597eae8bc5066a768]",
    "patternType": "stix",
    "validFrom": "2023-03-08T10:53:30Z",
    "validUntil": "2023-04-07T10:53:30Z"
  }
}
```

### Sample Response

```
{
  "errors": []
}
```

## Microsoft Azure Sentinel Delete Collection

The Microsoft Azure Sentinel Delete Collection action will delete the selected collection from Microsoft Azure Sentinel.



Since this Workflow it's only to delete a collection of Indicators from Microsoft Azure Sentinel, the action does not ingest any data back to the TQ Threat Library.

```
DELETE "https://management.azure.com/subscriptions/{{subscription_id}}/  
resourceGroups/{{resource_group}}/providers/Microsoft.OperationalInsights/  
workspaces/{{workspace}}/providers/Microsoft.SecurityInsights/  
threatIntelligence/main/indicators/{{indicator_name}}api-version=2021-10-01"
```

# Enriched Data



Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

## Microsoft Azure Sentinel Enrich Indicators

| METRIC               | RESULT    |
|----------------------|-----------|
| Run Time             | 2 minutes |
| Indicators           | 10        |
| Indicator Attributes | 40        |

## Microsoft Azure Sentinel Add Tag

| METRIC     | RESULT   |
|------------|----------|
| Run Time   | 1 minute |
| Indicators | 10       |

## Known Issues / Limitations

- The following is a known Microsoft Azure Sentinel API bug. Attempting to upload indicators that were previously deleted from the platform will result in an API error. The error states that you cannot update the indicators. This is due to the indicators still existing on the platform, in some format, despite being deleted.
- The function **Microsoft Azure Sentinel Export Collection** needs a STIX identifier for each indicator that is uploaded to Microsoft Sentinel. Right now this identifier is generated random.

# Change Log

- **Version 1.0.1**
  - Updated the API endpoint for the **Microsoft Azure Sentinel Export Collection** action.
  - Added a new Known Issue for the **Microsoft Azure Sentinel Export Collection** action.
  - Added support for the Microsoft logo. Installing the action bundle via the zip file will display the logo on the action details and orchestrator builder screens.
- **Version 1.0.0**
  - Initial release