

ThreatQuotient



ThreatQ Action Bundle for Microsoft Azure Sentinel

Version 1.0.5

August 12, 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	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Permissions.....	7
Configure New Application.....	7
Installation.....	8
Configuration	9
Enrich Indicators Action Parameters	9
Add Tag Action Parameters	11
Export Collection Action Parameters	13
Delete Collection Action Parameters	15
Defender ATP Export Collection Action Parameters.....	17
Create Incident Action Parameters	20
Export IOC Action Parameters	23
Actions	24
Microsoft Azure Sentinel Enrich Indicators	26
Microsoft Azure Sentinel Add Tag	29
Microsoft Azure Sentinel Export Collection	31
Microsoft Defender ATP Export Collection.....	32
Microsoft Azure Sentinel Delete Collection.....	35
Microsoft Azure Sentinel Create Incident.....	36
Microsoft Azure Sentinel Export IOC.....	37
API Mapping.....	38
Enriched Data.....	39
Microsoft Azure Sentinel Enrich Indicators	39
Microsoft Azure Sentinel Add Tag	39
Microsoft Azure Sentinel Create Incident.....	39
Known Issues / Limitations.....	40
Change Log	41

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

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	1.0.5
Compatible with ThreatQ Versions	>= 5.25.0
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 in the Threat Library against Microsoft Sentinel and enriches them with the returned data.
- **Microsoft Azure Sentinel Add Tag** - adds user defined tags to indicators in a data collection both in the Microsoft Sentinel context and in TQ.
- **Microsoft Azure Sentinel Export Collection** - queries indicators in the Threat Library against Microsoft Sentinel and adds them if not present.
- **Microsoft Azure Sentinel Export IOC** - exports indicators in the Threat Library to Microsoft Sentinel.
- **Microsoft Defender ATP Export Collection** - adds the indicators in the Threat Library to Microsoft Defender ATP.
- **Microsoft Azure Sentinel Delete Collection** - queries indicators in the Threat Library against Microsoft Sentinel and deletes them if present.
- **Microsoft Azure Sentinel Create Incidents** - uses ThreatQ objects to create incidents in Microsoft Sentinel.

The actions are compatible with the following object types:

- Campaigns
- Events
- Incidents
- Indicators
 - CIDR Block
 - Email Address
 - Filename
 - File Path
 - FQDN
 - IP Address
 - IPv6 Address
 - Mutex
 - URL
 - SHA-1
 - SHA-256
 - MD5

The actions return the following enriched system objects:

- Campaigns
 - Campaign Attributes
- Events
 - Event Attributes
- Incidents
 - Incident Attributes
- 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:
 - CIDR Block
 - Email Address
 - Filename
 - File Path
 - FQDN
 - IP Address
 - IPv6 Address
 - Mutex
 - URL
 - SHA-1
 - SHA-256
 - MD5
- [Proper Azure Permissions](#)
- [Application set up for Microsoft Azure](#)

Permissions

The integration requires the `ThreatIndicators.ReadWrite.OwnedBy` permission to be enabled for the ThreatQ Integration App, as both a **delegated right** as well as an **application right**.

Configure New Application

Before installing the integration on the ThreatQ side, you will need to configure a new application on Microsoft Azure. The following link will take you to Microsoft's documentation on how to connect Azure Sentinel to ThreatQ via an Azure Application. In the guide, you can skip step 4 as that step is handled by the ThreatQ integration.

<https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence#connect-azure-sentinel-to-your-threat-intelligence-platform>

Alternatively, you can follow the instructions from the link below, without skipping any of the steps:

<https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-tip#connect-azure-sentinel-to-your-threat-intelligence-platform>

Use the following steps if you select **Azure Sentinel** as the **Target** in the connector configuration settings.

<https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-upload-api>

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.

Enrich Indicators Action Parameters

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.

PARAMETER

DESCRIPTION

Workspace Name

The name of the workspace, obtained from the Log Analytics Workspaces.

Objects Per Run

The max number of objects for the action to submit per run.

< Microsoft Azure Sentinel Enrich Indicators



Uninstall

Additional Information

Integration Type: Action

Version: 1

Action ID: 5

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

Objects Per Run

The max number of objects to send to this action, per run.

Save

Add Tag Action Parameters

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).
Objects Per Run	The max number of objects for the action to submit per run.

< Microsoft Azure Sentinel Add Tag



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 8

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

This is obtained from the Log Analytics Workspaces

Tags

List of tags to be appended (split by a comma)

Objects Per Run

The max number of objects to send to this action, per run.

Export Collection Action Parameters

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.
Default Expiration Days	Enter the number of days the indicators remain valid.
Hostname	Your ThreatQ Hostname.
Related Context Filter	Select the pieces of context that should be exported.
Default Threat Type	Select the default threat type to apply to the exported IOCs if no suitable attribute exists.  The Default Threat Type value can be overwritten by adding an indicator attribute whose value is a valid Threat Type value (based on the above options for Default

PARAMETER	DESCRIPTION
	Threat Type) or is an alias of a valid Threat Type based on the following mapping: <pre>aliases = { 'C2': ['command and control', 'c&c', 'command & control'], 'DDoS': ['denial of service'], 'CryptoMining': ['crypto', 'mining', 'crypto miner'], 'Botnet': ['bot'] }</pre>
Always use the selected Default Threat Type	Enable this field to always use the Default Threat Type selected above.
Objects Per Run	The max number of objects for the action to submit per run.

< Microsoft Azure Sentinel Export Collection



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 6

Accepted Data Types:

Indicators

- CIDR Block
- Email Address
- Filename
- File Path
- FQDN
- IP Address
- IPv6 Address
- Mutex
- MDS
- SHA-1
- SHA-256
- URL

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

This is obtained from the Log Analytics Workspaces

Workspace ID

This is obtained from the Log Analytics Workspaces

Default Expiration Days

Delete Collection Action Parameters

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.
Objects Per Run	The max number of objects for the action to submit per run.

< Microsoft Azure Sentinel Delete Collection



Uninstall

Additional information

Integration Type: Action

Version:

Action ID: 9

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

Objects Per Run

The max number of objects to send to this action, per run.

Save

Defender ATP Export Collection Action Parameters

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.
Action	The action to take when an IOC is observed in your environment. Options include: ◦ Unknown ◦ Allow ◦ Block ◦ Alert
Default Severity	The default severity to apply to the exported IOCs if attribute Severity is not present. The range available is 0 - 5.  The Default Severity value can be overwritten by adding an indicator attribute whose name is Severity and whose value is between 0-5 (inclusive).
Default Expiration Days	Enter the number of days the indicators remain valid.
Hostname	Your ThreatQ Hostname.
Default Threat Type	Select the default threat type to apply to the exported IOCs if no suitable attribute exists. Options include: ◦ Botnet ◦ C2 ◦ MaliciousUrl ◦ Malware

PARAMETER	DESCRIPTION
	◦ Compromised ◦ CryptoMining ◦ Darknet ◦ DDoS ◦ Phishing ◦ Proxy ◦ PUA ◦ WatchList  The Default Threat Type value can be overwritten by adding an indicator attribute whose value is a valid Threat Type value (based on the above options for Default Threat Type) or is an alias of a valid Threat Type based on the following mapping: <pre>aliases = { 'C2': ['command and control', 'c&c', 'command & control'], 'DDoS': ['denial of service'], 'CryptoMining': ['crypto', 'mining', 'crypto miner'], 'Botnet': ['bot'] }</pre>
Always use the selected Default Threat Type	Enable this parameter to configure the action to always use the Default Threat Type selected above.
Related Context Filter	Select the pieces of context that should be exported. Options include: ◦ Indicator Descriptions ◦ Malware Family Attribute ◦ Attributes Having Valid Kill Chain Phases ◦ Related Adversaries
Behavior for URL indicators without a scheme defined	Defines how data collection URL indicators should be handled. Microsoft needs a scheme (http/https) defined for URL indicators. Options include: ◦ Skip Indicators ◦ Add "http" ◦ Add "https"
Objects Per Run	The max number of objects for the action to submit per run.

< Microsoft Defender ATP Export Collection



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 7

Accepted Data Types:

Indicators

- CIDR Block
- Email Address
- Filename
- File Path
- FQDN
- IP Address
- IPv6 Address
- Mutex
- MDS
- SHA-1
- SHA-256
- URL

Configuration

Tenant ID

Microsoft Active Directory App's Tenant ID

Client ID

Microsoft Active Directory App's Client ID

Client Secret

Microsoft Active Directory App's Client Secret

Action

Block

The action to take when an IOC is observed in your environment

Default Severity

3

The default severity to apply to the exported IOCs.

Default Expiration Days

30

How many days should these indicators remain valid

Hostname

ThreatQ Hostname

Default Threat Type

WatchList

Create Incident Action Parameters

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.
Severity	The action to take when an IOC is observed in your environment. Options include: ◦ Unknown ◦ Allow ◦ Block ◦ Alert
Status	The status of the incident that will be created. Options include: ◦ New ◦ Active ◦ Closed
Classification	Select the reason for closing the incident. Options include: ◦ Benign Positive ◦ False Positive ◦ True Positive

PARAMETER	DESCRIPTION
	◦ Undetermined  This parameter will only be available if you selected Closed as your Status.
Classification Comment	Enter a reason for closing the incident.  This parameter will only be available if you selected Closed as your Status.
Classification Reason	Select the classification reason for why the incident was closed. Options include: ◦ Inaccurate Data ◦ Incorrect Alert Logic ◦ Suspicious Activity ◦ Suspicious But Expected  This parameter will only be available if you selected Closed as your Status.
Owner Email	The email of user the incident will be assigned to.
Objects Per Run	The max number of objects for the action to submit per run.

← Microsoft Azure Sentinel Create Incident



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Campaign

Events

Incident

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

This is obtained from the Log Analytics Workspaces

Severity

Informational

The severity of the incident

Status

New

Export IOC Action Parameters

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.
Workspace ID	The ID of the workspace, obtained from the Log Analytics Workspaces.
Default Expiration Days	Enter the number of days the indicators remain valid.
Hostname	Your ThreatQ Hostname.
Objects Per Run	The max number of objects for the action to submit per run.

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

Actions

The following actions are available:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Microsoft Azure Sentinel Enrich Indicators	Enrich Indicators with attributes.	Indicators	CIDR Block, Email Address, Filename, File Path, IP Address, IPv6 Address, Mutex, URL, FQDN, MD5, SHA-256, SHA-1
Microsoft Azure Sentinel Add Tag	Add custom tags to the Indicators.	Indicators	CIDR Block, Email Address, Filename, File Path, IP Address, IPv6 Address, Mutex, URL, FQDN, MD5, SHA-256, SHA-1
Microsoft Azure Sentinel Export Collection	Add Indicators to Microsoft Azure Sentinel.	Indicators	CIDR Block, Email Address, Filename, File Path, IP Address, IPv6 Address, Mutex, URL, FQDN, MD5, SHA-256, SHA-1
Microsoft Defender ATP Export Collection	Add Indicators to Microsoft Defender ATP.	Indicators	CIDR Block, Email Address, Filename, File Path, IP Address, IPv6 Address, Mutex, URL, FQDN, MD5, SHA-256, SHA-1
Microsoft Azure Sentinel Delete Collection	Delete Indicators from Microsoft Azure Sentinel.	Indicators	CIDR Block, Email Address, Filename, File Path, IP Address, IPv6 Address, Mutex, URL, FQDN, MD5, SHA-256, SHA-1
Microsoft Azure Sentinel Create Incident	Creates Incidents in Microsoft Azure Sentinel.	Campaigns, Events, Incidents	N/A
Microsoft Azure Sentinel Export IOC	Add Indicators to Microsoft Azure Sentine.	Indicators	CIDR Block, Email Address, Filename, File Path, IP Address,

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
			IPv6 Address, Mutex, URL, FQDN, MD5, SHA-256, SHA-1

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 TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value[].properties.description	Indicator.Description	N/A	N/A	IOC exported from ThreatQ	N/A
.value[].properties.threatIntelligenceTags	Indicator.Tag	N/A	N/A	tg1	N/A
.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 Export collection action will upload the indicators from the selected collection to Microsoft Sentinel Threat Intelligence Portal. This action only pushes a collection of Indicators to Microsoft Azure Sentinel and does not ingest anything back to the ThreatQ Threat Library.

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



The Default Threat Type value can be overwritten by adding an indicator attribute whose value is a valid Threat Type value (based on the above options for Default Threat Type) or is an alias of a valid Threat Type based on the following mapping:

```
aliases = {
  'C2': ['command and control', 'c&c', 'command & control'],
  'DDoS': ['denial of service'],
  'CryptoMining': ['crypto', 'mining', 'crypto miner'],
  'Botnet': ['bot']
}
```

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 Defender ATP Export Collection

The Microsoft Defender ATP Export Collection action will upload the indicators from the selected collection to Microsoft Defender ATP.

POST "https://graph.microsoft.com/beta/security/tiIndicators/
submitTiIndicators"

Sample Body:

Form URL-Encoded

```
{
  "value": [
    {
      "azureTenantId": "{{TENANT_ID}}",
      "action": "Block",
      "description": "IOC exported from ThreatQ.",
      "labels": [
        "tag1"
      ],
      "lastReportedDateTime": "2023-03-08T10:53:30Z",
      "isActive": true,
      "externalId": "79",
      "confidence": 70,
      "threatType": "WatchList",
      "targetProduct": "Microsoft Defender ATP",
      "expirationDateTime": "2023-06-08T10:53:30Z",
      "severity": 3,
      "killChain": [
        "Delivery"
      ],
      "additionalInformation": "{{THREATQ_HOSTNAME}}/indicators/79/
details",
      "malwareFamilyNames": [
        "Trojan"
      ],
      "activityGroupNames": [
        "APT40"
      ],
      "fileHashValue": "008b81f89405228597eae8bc5066a768",
      "fileHashType": "md5"
    }
  ]
}
```

Sample Response:

```
{
  "@odata.context": "https://graph.microsoft.com/beta/
$metadata#Collection(microsoft.graph.tiIndicator)",
  "value": [
```



```
{
  "action": "block",
  "activityGroupNames": [],
  "additionalInformation": "{{THREATQ_HOSTNAME}}/indicators/79/details",
  "azureTenantId": "TENANT_ID",
  "confidence": 70,
  "description": "IOC exported from ThreatQ",
  "diamondModel": null,
  "domainName": null,
  "emailEncoding": null,
  "emailLanguage": null,
  "emailRecipient": null,
  "emailSenderAddress": null,
  "emailSenderName": null,
  "emailSourceDomain": null,
  "emailSourceIpAddress": null,
  "emailSubject": null,
  "emailXMailer": null,
  "expirationDateTime": "2023-06-08T10:53:30Z",
  "externalId": "7275",
  "fileCompileDateTime": null,
  "fileCreatedDateTime": null,
  "fileHashType": "md5",
  "fileHashValue": "008b81f89405228597eae8bc5066a768",
  "fileMutexName": null,
  "fileName": null,
  "filePacker": null,
  "filePath": null,
  "fileSize": null,
  "fileType": null,
  "id": "34636",
  "ingestedDateTime": null,
  "isActive": true,
  "killChain": [],
  "knownFalsePositives": null,
  "lastReportedDateTime": "2023-03-08T10:53:30Z",
  "malwareFamilyNames": [],
  "networkCidrBlock": null,
  "networkDestinationAsn": null,
  "networkDestinationCidrBlock": null,
  "networkDestinationIPv4": null,
  "networkDestinationIPv6": null,
  "networkDestinationPort": null,
  "networkIPv4": null,
  "networkIPv6": null,
  "networkPort": null,
  "networkProtocol": null,
  "networkSourceAsn": null,
  "networkSourceCidrBlock": null,
  "networkSourceIPv4": null,
```

```
    "networkSourceIPv6": null,  
    "networkSourcePort": null,  
    "passiveOnly": null,  
    "severity": 3,  
    "tags": [],  
    "targetProduct": "Microsoft Defender ATP",  
    "threatType": "WatchList",  
    "tlpLevel": null,  
    "url": null,  
    "userAgent": null,  
    "vendorInformation": null  
  }  
]  
}
```

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"
```

Microsoft Azure Sentinel Create Incident

The Microsoft Azure Sentinel Create Incident action uses ThreatQ objects to create incidents in Microsoft Sentinel.

```
POST "https://management.azure.com/subscriptions/{{subscription_id}}/resourceGroups/{{resource_group}}/providers/Microsoft.OperationalInsights/workspaces/{{workspace}}/providers/Microsoft.SecurityInsights/incidents/main/tq_{{object_type}}_{{id}}?api-version=2024-03-01"
```

Sample Body:

```
{
  "properties": {
    "severity": "High",
    "status": "Closed",
    "title": "Grandoreiro",
    "description": "Grandoreiro is a major cybersecurity threat.",
    "labels": [
      "malware"
    ],
    "firstActivityTimeUtc": "2024-03-14T08:23:00Z",
    "lastActivityTimeUtc": "2024-04-01T08:23:00Z",
    "classification": "FalsePositive",
    "classificationComment": "Incident investigation was finished.",
    "classificationReason": "InaccurateData",
    "owner": {
      "email": "user1@threatq.onmicrosoft.com"
    }
  }
}
```

Sample Response:

```
{
  "id": "/subscriptions/f1c10b41-49ff-4791-b366-b3bbb37fca4c/resourceGroups/group1/providers/Microsoft.OperationalInsights/workspaces/tqsentinal/providers/Microsoft.SecurityInsights/Incidents/tq_incident_601",
  "name": "tq_incident_601",
  "etag": "\"05007801-0000-0100-0000-660e51af0000\"",
  "type": "Microsoft.SecurityInsights/Incidents",
  "properties": {
    "title": "Grandoreiro",
    "description": "Grandoreiro is a major cybersecurity threat.",
    "severity": "Hign",
    "status": "Closed",
    "classification": "FalsePositive",
    "classificationReason": "InaccurateData",
  }
}
```

```

"classificationComment": "Incident investigation was finished.",
"owner": {
  "objectId": null,
  "email": "user1@threatq.onmicrosoft.com",
  "assignedTo": null,
  "userPrincipalName": null,
  "ownerType": "Unknown"
},
"labels": [
  {
    "labelName": "malware",
    "labelType": "User"
  }
],
"firstActivityTimeUtc": "2024-03-14T08:23:00Z",
"lastActivityTimeUtc": "2024-04-01T08:23:00Z",
"lastModifiedTimeUtc": "2024-04-01T08:23:00Z",
"createdTimeUtc": "2024-03-14T08:23:00Z",
"incidentNumber": 25529,
"additionalData": {
  "alertsCount": 0,
  "bookmarksCount": 0,
  "commentsCount": 0,
  "alertProductNames": [],
  "tactics": [],
  "techniques": []
},
"relatedAnalyticRuleIds": [],
"incidentUrl": "https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Incident/subscriptions/f1c10b41-49ff-4791-b366-b3bbb37fca4c/resourceGroups/group1/providers/Microsoft.OperationalInsights/workspaces/tqsentinal/providers/Microsoft.SecurityInsights/Incidents/tq_incident_601",
"providerName": "Azure Sentinel",
"providerIncidentId": "25529"
}
}

```

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.incidentUrl	Campaign/Event/ Incident.Attribute	Azure Incident URL	N/A	https:// portal.azure.com...	N/A

Microsoft Azure Sentinel Export IOC

The Microsoft Azure Sentinel Export IOC action will upload the indicators from the selected collection to Microsoft Sentinel Threat Intelligence Portal.

API Mapping

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

Sample Body

Form URL-Encoded

```
{
  "SourceSystem": "Azure Sentinel",
  "Value": [
    {
      "id": "indicator--e6493692-e007-3274-97c3-39c2a2f02994",
      "type": "indicator",
      "name": "Custom Threat Intelligenc",
      "spec_version": "2.1",
      "confidence": 70,
      "pattern": "[file:hashes.'MD5' =  
'008b81f89405228597eae8bc5066a768']",
      "pattern_type": "stix",
      "valid_from": "2023-03-08T10:53:30Z",
      "created": "2023-03-08T10:53:30Z",
      "modified": "2023-03-08T10:53:30Z",
      "external_references": [
        {
          "source_name": "ThreatQ",
          "external_id": 79,
          "url": "{{THREATQ_HOSTNAME}}/indicators/79/details"
        }
      ]
    }
  ]
}
```

Sample Response

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



Since this action only pushes a collection of Indicators to Microsoft Azure Sentinel and does not ingest anything back to the ThreatQ Threat Library.

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

Microsoft Azure Sentinel Create Incident

METRIC	RESULT
Run Time	1 minute
Incidents	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 1.0.5**
 - Resolved an issue where actions applied the wrong source name to objects.
- **Version 1.0.4**
 - Added a new action: **Microsoft Azure Sentinel Export IOC**.
- **Version 1.0.3**
 - Added a new action: **Microsoft Azure Sentinel Create Incident**.
 - Updated the minimum ThreatQ version to 5.25.0.
- **Version 1.0.2**
 - Added support for the following indicator types: CIDR Block, Email Address, Filename, File Path, IPv6 Address, Mutex, and SHA-1.
 - Added the ability to collection export more information using the Microsoft Azure Sentinel Export Collection action. New parameters include:
 - Related Context Filter
 - Default Threat Type
 - Always use the selected Default Threat Type
 - Added a new action: **Microsoft Defender ATP Export Collection**. This action allows users to export indicators to Microsoft Defender ATP.
- **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