ThreatQuotient

ThreatQ CDF for Microsoft Azure Sentinel Incidents

Version 1.2.2

January 14, 2025

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	1.2.2
Compatible with ThreatQ Versions	>= 4.37.0
Support Tier	ThreatQ Supported

Introduction

Sentinel is a project of **Microsoft Azure** with the goal of alerting SOCs of potential compromise. The ThreatQ CDF for Microsoft Azure Sentinel Incidents retrieves those incidents.

The Microsoft Azure Sentinel Incidents CDF provides the following feeds:

- **Microsoft Azure Sentinel Incidents** - retrieves a list of incidents.
- **Microsoft Azure Sentinel - Authentication (supplemental)** - authenticates against Sentinel.
- **Microsoft Azure Sentinel - Incidents Relations (supplemental)** - retrieves all relations for a given incident.
- **Microsoft Azure Sentinel - Entity Details (supplemental)** - retrieves context for each entity related to an incident in the incident list by expanding the entity.
- **Microsoft Azure Sentinel - Entity Indicators (supplemental)** - retrieves a list of indicators, emails, malware and attributes for each entity related to an incident in the incident list.

The integration ingests the following system objects into the ThreatQ platform:

- Incidents
- Indicators

To acquire required app permissions, the app registration must have the proper API permissions. See the Prerequisites section for more details.

The scope for authentication is `https://management.azure.com/.default` which means non-standard practices for authentication are required.

Prerequisites

The following is required in order to install and configure the integration.

1. Register your ThreatQ integration for the Azure portal - see https://learn.microsoft.com/en-us/azure/azure-monitor/logs/api/register-app-for-token for more details and instructions.
2. Apply Graph API permissions.
3. Apply the Microsoft Contributor Role.
4. Locate all required credentials for the configuration page.

Applying Graph API Permissions

1. Navigate to your Azure App Registrations portal and open the ThreatQ integration app.

   > You can also search for `App Registrations` and then select the first option.

2. Open the ThreatQ integration App's configuration page.
3. Open the **API Permissions** tab located on the sidebar.
4. Click on the **Add a Permission** button.
5. Select the **Microsoft Graph** API.
6. Click on the **Application Permissions** option.
7. Search for `ThreatIndicators` and enable the `ThreatIndicators.ReadWrite.OwnedBy` entry.
8. Search for `SecurityAlert` and enable the `SecurityAlert.ReadWrite.All` entry.
9. Click on **Add Permissions** to add the two entries that have been enabled.

Applying the Microsoft Contributor Role

1. Navigate to your Azure App Registrations portal and open the Log Analytics workspace.

   > You can also search for `Log Analytics workspaces` and then select the first option.

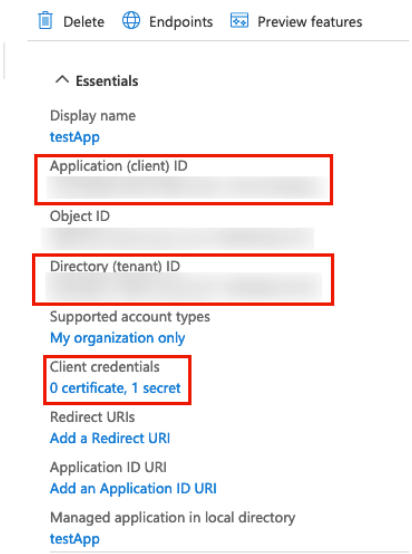
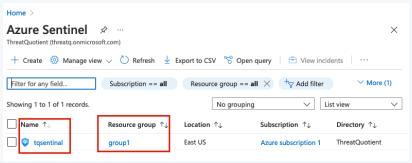
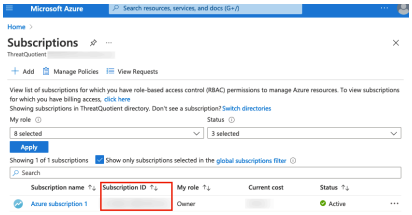
2. Open the workspace that contains your Microsoft Sentinel instance.
3. Click on the **Access Control (IAM)** tab.
4. Click on the **Add** dropdown and select the **Add Role Assignment** option.
5. Search for `Microsoft Sentinel Contributor` in the Add Role wizard and then click on **Next**.
6. Click on the **Select Members** button to open the search modal.
7. Use the search modal to search for your ThreatQ app registration.
8. Use the **Select** button to select the ThreatQ app.
9. Click on the **Review + Assign** button.
10. Review the assignment and then click on the **Review + Assign** button again.

11. You will now be able to see the role assignment you just added.

> This information will not be accessible from the App's configuration page.

Required Credential Locations

The integration requires the following values when configuring the feeds:

PARAMETER	DESCRIPTION	EXAMPLE
Tenant ID	The Tenant ID can be found under Azure Services > App Registration > Your App name.	
Application (client) ID	The Application (client) ID can be found under Azure Services > App Registration > Your App name.	
Client Secret	The Client Secret can be found under Azure Services > App Registration > Your App name.	
Workspace & Resource Group	The Workspace & Resource Group can be found under Azure Sentinel.	
Subscription ID	The Subscription ID can be found by clicking on the Subscriptions option under the Azure Services heading on the main Microsoft Azure landing page.	

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 feed(s) 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.

7. The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed.

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:

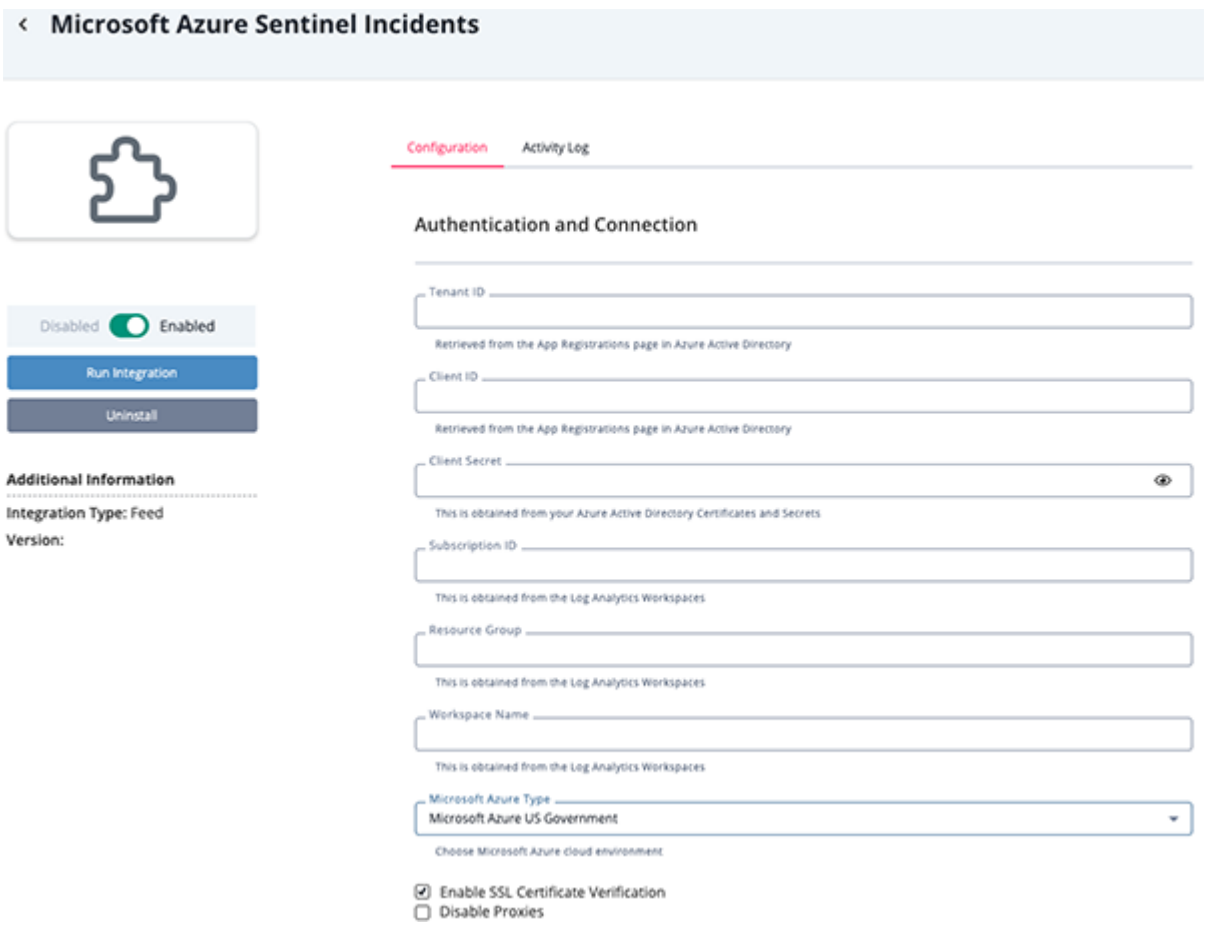
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   > 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
Tenant ID	The Tenant ID can be found under Azure Services > App Registration > Your App name.
Client ID	The Application (client) ID can be found under Azure Services > App Registration > Your App name.
Client Secret	The Client Secret can be found under Azure Services > App Registration > Your App name.
Subscription ID	The Subscription ID can be found by clicking on the Subscriptions option under the Azure Services heading on the main Microsoft Azure landing page.
Resource Group	The Resource Group can be found under Azure Sentinel.
Workspace Name	The Workspace can be found under Azure Sentinel.
Microsoft Azure Type	Select the Microsoft Azure cloud environment. Options include: ◦ Microsoft Azure Global ◦ Microsoft Azure US Government

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Severity	The severity of the incidents. Options include: ◦ High ◦ Medium ◦ Low ◦ Unknown ◦ Informational You can select more than option severity option.



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

Microsoft Azure Sentinel - Authentication (supplemental)

Supplemental feed which authenticates against Sentinel.

`POST https://login.microsoftonline.com/{tenant_id}/oauth2/v2.0/token`

Sample Response:

```
{
    "token_type": "Bearer",
    "expires_in": 3599,
    "ext_expires_in": 3599,
    "access_token": "This would be your access token"
}
```

Microsoft Azure Sentinel Incidents

Retrieves a list of incidents.

```
GET https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/providers/Microsoft.SecurityInsights/incidents?api-version=2021-04-01&$filter=(properties/lastModifiedTimeUtc ge {since} and properties/lastModifiedTimeUtc le {until})&$top=100
```

Sample Response:


```
{
  "value": [
    {
      "id": "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXX/providers/Microsoft.SecurityInsights/incidents/73e01a99-5cd7-4139-a149-9f2736ff2ab5",
      "name": "73e01a99-5cd7-4139-a149-9f2736ff2ab5",
      "type": "Microsoft.SecurityInsights/incidents",
      "etag": "\"0300bf09-0000-0000-0000-5c37296e0000\"",
      "properties": {
        "lastModifiedTimeUtc": "2019-01-01T13:15:30Z",
        "createdTimeUtc": "2019-01-01T13:15:30Z",
        "lastActivityTimeUtc": "2019-01-01T13:05:30Z",
        "firstActivityTimeUtc": "2019-01-01T13:00:30Z",
        "description": "This is a demo incident",
        "title": "My incident",
        "owner": {
          "objectId": "2046feea-040d-4a46-9e2b-91c2941bfa70",
          "email": "john.doe@contoso.com",
          "userPrincipalName": "john@contoso.com",
          "assignedTo": "john doe"
        },
        "severity": "High",
        "classification": "FalsePositive",
        "classificationComment": "Not a malicious activity",
        "classificationReason": "IncorrectAlertLogic",
        "status": "Closed",
        "incidentUrl": "https://portal.azure.com/#icon/Microsoft_Azure_Security_Insights/Incident/subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXXX/providers/Microsoft.SecurityInsights/incidents/73e01a99-5cd7-4139-a149-9f2736ff2ab5",
        "incidentNumber": 3177,
        "labels": [],
        "relatedAnalyticRuleIds": [
          "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXXX/providers/
```

```
Microsoft.SecurityInsights/alertRules/fab3d2d4-747f-46a7-8ef0-9c0be8112bf7",
          "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/
XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXXX/providers/
Microsoft.SecurityInsights/alertRules/8deb8303-e94d-46ff-96e0-5fd94b33df1a"
        ],
        "additionalData": {
          "alertsCount": 0,
          "bookmarksCount": 0,
          "commentsCount": 3,
          "alertProductNames": [],
          "tactics": [
            "Persistence"
          ]
        }
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
'Sentinel Incident' + .value[].properties. incidentNumber + ':' + .properties. alertDisplayName + '(Alerts:' + .value[].properties. additionalData.alertsCount + ')'	Incident. Value	N/A	.value[].properties. createdTimeUtc	Sentinel Incident 3177: High Severity (Alerts: 1))	.properties.alertDisplayName is obtained by Microsoft Azure Sentinel - Entity Details supplemental feed
.value[].properties.description	Incident. Description	N/A	.value[].properties. createdTimeUtc	This is a demo incident	N/A
.value[].properties. firstActivityTimeUtc	Incident. Started_at	N/A	.value[].properties. createdTimeUtc	08/18/2021 12:30	N/A
.value[].properties. lastActivityTimeUtc	Incident. Ended_at	N/A	.value[].properties. createdTimeUtc	08/18/2021 12:43	N/A
.value[].properties. additionalData.alertsCount	Incident. Attribute	Alert Count	.value[].properties. createdTimeUtc	10	N/A
.value[].properties.severity	Incident. Attribute	Severity	.value[].properties. createdTimeUtc	High	N/A
.value[].properties. incidentUrl	Incident. Attribute	Incident URL	.value[].properties. createdTimeUtc	https:// portal.azure.com/ #asset/ Microsoft_Azure_ Security_Insights/ Incident/ subscriptions/ XXXXXXXX-XX XX-XXXX-XXXX- XXXXXXXXXXXX/ resourceGroups/XXXX/ provi ders/ Microsoft.Operationall nsights/workspaces/ XXXXX/ providers/ Microsoft.Securit yInsights/incidents/ 73e01a99-5cd7-4139- a149-9f2736ff2ab5	N/A
.value[].properties. owner.assignedTo	Incident. Attribute	Assigned to	.value[].properties. createdTimeUtc	John Doe	N/A
.value[].properties.status	Incident. Attribute	Status	.value[].properties. createdTimeUtc	Closed	N/A

In order to call the Microsoft Azure Sentinel - Incidents Relations supplemental feed `.value[].name` is used as `incidentId` parameter.

Microsoft Azure Sentinel - Incidents Relations (supplemental)

Supplemental feed which retrieves all relations for a given incident.

```
GET https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/
{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/
{workspaceName}/providers/Microsoft.SecurityInsights/incidents/{incidentId}/
relations?api-version=2019-01-01-preview
```

Sample Response:

```
{
  "value": [
      {
        "id": "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/
XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXXX/providers/
Microsoft.SecurityInsights/Incidents/f081eba2-c310-0205-f3b3-0a719f1094f5/
relations/f081eba2-c310-0205-f3b3-0a719f1094f5_802422ee-e1ea-
f8d3-089e-338e66ad265e",
        "name": "f081eba2-c310-0205-f3b3-0a719f1094f5_802422ee-e1ea-
f8d3-089e-338e66ad265e",
        "type": "Microsoft.SecurityInsights/Incidents/relations",
        "properties": {
            "relatedResourceId": "/subscriptions/XXXXXXXX-XXXX-XXXX-
XXXXXXXXXXXX/resourceGroups/XXXX/providers/Microsoft.OperationalInsights/
workspaces/XXXXX/providers/Microsoft.SecurityInsights/entities/802422ee-e1ea-
f8d3-089e-338e66ad265e",
            "relatedResourceName": "802422ee-e1ea-f8d3-089e-338e66ad265e",
            "relatedResourceType": "Microsoft.SecurityInsights/entities",
            "relatedResourceKind": "SecurityAlert"
        }
    }
  ]
```

The `.value[].properties.relatedResourceName` is used as the `relatedResourceName` request parameter in order to call the supplemental feeds Microsoft Azure Sentinel - Entity Details and Microsoft Azure Sentinel - Entity Indicators.

Microsoft Azure Sentinel - Entity Details (supplemental)

Supplemental feed which retrieves context for each entity related to an incident in the incident list by expanding the entity.

```
GET https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/
{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/
{workspaceName}/providers/Microsoft.SecurityInsights/entities/
{relatedResourceName}?api-version=2019-01-01-preview
```

Sample Response:

```
{
    "id": "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/XXXX/
providers/Microsoft.OperationalInsights/workspaces/XXXXX/providers/
Microsoft.SecurityInsights/entities/aa0a26dd-c7c9-03f7-8ba9-e226e5772d0b",
    "name": "aa0a26dd-c7c9-03f7-8ba9-e226e5772d0b",
    "type": "Microsoft.SecurityInsights/entities",
    "kind": "SecurityAlert",
    "properties": {
        "systemAlertId": "aa0a26dd-c7c9-03f7-8ba9-e226e5772d0b",
        "tactics": [],
        "alertDisplayName": "Sighting of Malicious Indicators",
        "confidenceLevel": "Unknown",
        "severity": "High",
        "vendorName": "Microsoft",
        "productName": "Azure Sentinel",
        "productComponentName": "Scheduled Alerts",
        "alertType": "eaa0f854-9594-4ac3-8891-
b4d7fb966789_2ea93a41-39d3-4f9e-81c3-339048aff576",
        "processingEndTime": "2021-08-10T22:59:40.5744836Z",
        "status": "New",
        "endTimeUtc": "2021-08-08T00:38:44.054Z",
        "startTimeUtc": "2021-08-08T00:38:44.007Z",
        "timeGenerated": "2021-08-10T22:59:40.5744861Z",
        "providerAlertId": "8a4eee51-b105-432d-aba1-f1866eb820cb",
        "resourceIdentifiers": [
            {
                "type": "LogAnalytics",
                "workspaceId": "eaa0f854-9594-4ac3-8891-b4d7fb966789"
            }
        ],
        "additionalData": {
            "ProcessedBySentinel": "True",
            "Alert generation status": "Full alert created",
            "Search Query Results Overall Count": "103",
            "Query Start Time UTC": "2021-08-07T22:54:31Z",
            "Query End Time UTC": "2021-08-10T22:54:31Z",
            "Analytic Rule Name": "Sighting of Malicious Indicators",
            "Analytic Rule Ids": "[\"2ea93a41-39d3-4f9e-81c3-339048aff576\"]",
```

```
            "Trigger Threshold": "0",
            "Trigger Operator": "GreaterThan",
            "Event Grouping": "SingleAlert",
            "Correlation Id": "eaa0f854-9594-4ac3-8891-
b4d7fb966789_2ea93a41-39d3-4f9e-81c3-339048aff576_637642331713403654",
            "Data Sources": "[\"tqsentinal\"]",
            "Query Period": "3.00:00:00",
            "Query": "// The query_now parameter represents the time (in UTC)
at which the scheduled analytics rule ran to produce this alert.\r\nset
query_now = datetime(2021-08-10T22:54:31.3403654Z);
\r\nThreatIntelligenceIndicator\n| where ExpirationDateTime > now() and
ThreatSeverity >= 5\n| extend HostCustomEntity = DomainName\n| extend
IPCustomEntity = NetworkIP\n| extend URLCustomEntity = Url",
            "Total Host Entities": "26",
            "Total IP Entities": "34"
        },
        "friendlyName": "Sighting of Malicious Indicators"
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.properties.confidenceLevel	Incident.Attribute	Confidence	incident .properties.createdTimeUtc	Unknown	N/A
.properties.vendorName	Incident.Attribute	Vendor	incident .properties.createdTimeUtc	Microsoft	N/A
.properties.productName	Incident.Attribute	Product	incident .properties.createdTimeUtc	Azure Sentinel	N/A
.properties.productComponentName	Incident.Attribute	Component	incident .properties.createdTimeUtc	Scheduled Alerts	N/A
.properties.tactics[]	Incident.Attribute	Tactic	incident .properties.createdTimeUtc	Persistence	N/A

Microsoft Azure Sentinel - Entity Indicators (supplemental)

Supplemental feed which retrieves a list of indicators, emails, malware and attributes for each entity related to an incident in the incident list.

> The request is always sent with the `expansionId` "98b974fd-cc64-48b8-9bd0-3a209f5b944b", which critical to the functionality of the integration.

```
POST https://management.azure.com/subscriptions/{subscriptionId}/
resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/
workspaces/{workspaceName}/providers/Microsoft.SecurityInsights/entities/
{relatedResourceName}/expand?api-version=2019-01-01-preview
```

Sample Response:

```
{
    "value": {
        "entities": [
            {
                "id": "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX/
resourceGroups/XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXXX/
providers/Microsoft.SecurityInsights/entities/aa4032d4-4fb4-9064-
dce3-1eb114077cb3",
                "name": "aa4032d4-4fb4-9064-dce3-1eb114077cb3",
                "type": "Microsoft.SecurityInsights/entities",
                "kind": "Host",
                "properties": {
                    "dnsDomain": "cn",
                    "hostName": "ribomoon",
                    "friendlyName": "ribomoon"
                }
            },
            {
                "id": "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXX/
resourceGroups/XXXX/providers/Microsoft.OperationalInsights/workspaces/XXXXX/
providers/Microsoft.SecurityInsights/entities/e8f1c440-a0f7-baea-e47a-
bb2fa60f25a8",
                "name": "e8f1c440-a0f7-baea-e47a-bb2fa60f25a8",
                "type": "Microsoft.SecurityInsights/entities",
                "kind": "Host",
                "properties": {
                    "dnsDomain": "space",
                    "hostName": "gtdspr",
                    "friendlyName": "gtdspr"
                }
            }
        ]
```

```
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value.entities[].properties.netBiosName	Indicator.Value	FQDN	N/A	NOR-TH-DC01.norbord.com	Applicable if .value.entities[].properties.kind = 'Host'
.value.entities[].properties.hostName + .value.entities[].properties.dnsDomain	Indicator.Value	FQDN	N/A	pcdcdctw01.westfrasertimber.ca	Applicable if .value.entities[].properties.kind = 'Host'
.value.entities[].properties.domainName	Indicator.Value	FQDN	N/A	nrghstsrwtrs.re	Applicable if .value.entities[].properties.kind = 'DnsResolution'
.value.entities[].properties.address	Indicator.Value	IP Address	N/A	99.86.37.27	Applicable if .value.entities[].properties.kind = 'Ip'
.value.entities[].properties.fileName	Indicator.Value	Filename	N/A	optisbr.exe	Applicable if .value.entities[].properties.kind = 'File'
.value.entities[].properties.url	Indicator.Value	URL	N/A	www.endmemo.com/sconvert/millionbillion.php	Applicable if .value.entities[].properties.kind = 'Url'
.value.entities[].properties.friendlyName	Indicator.Value	String	N/A	"msvsmon.exe" /__dbgautolaunch 0x00002DAC 0x66d4 /hostname [::1] /port 54628 /__pseudoremote	Applicable if .value.entities[].properties.kind = 'Process'
Azure Resource: .value.entities[].properties.resourceId	Indicator.Value	String	N/A	AZRP-RG-SECURITYTEAM/providers/Microsoft.Compute/virtualMachines/AZRP-VM-MISP001	Applicable if .value.entities[].properties.kind = 'AzureResource'
.value.entities[].properties.key	Indicator.Value	Registry Key	N/A	N/A	Applicable if .value.entities[].properties.kind = 'RegistryKey'
.value.entities[].properties.ntDomain+'\'+properties.accountName+'@'+properties.upnSuffix	Indicator.Value	Username	N/A	westfrasertimber\SADKIN1@westfraser.com	Applicable if .value.entities[].properties.kind = 'Account'
.value.entities[].properties.directory	Indicator.Value	File Path	N/A	c:\users\bselz\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\localstate\files\s0\3\attachments	Applicable if .value.entities[].properties.kind = 'File'
.value.entities[].properties.hashValue	Indicator.Value	.value.entities[].properties.algorithm	N/A	dd399ae46303343f9f0da189aee11c67bd868222	The hash type is determined by mapping .value.entities[].properties.algorithm through the Hash Type Mapping table below

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value.entities[].properties.mailboxPrimaryAddress	Indicator.Value	Email Address	N/A	pcdcdctw01.westfrastertimber.ca	Applicable if .value.entities[].properties.kind = 'Mailbox'
.value.entities[].properties.p1Sender	Indicator.Value	Email Address	N/A	naxxf@begc.ne	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.p2Sender	Indicator.Value	Email Address	N/A	naxxf@begc.ne	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.senderIP	Indicator.Value	Email Address	N/A	99.86.37.27	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.p1SenderDisplayName	Indicator.Attribute	Sender Display Name (P1)	N/A	john doe	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.p2SenderDisplayName	Indicator.Attribute	Sender Display Name (P2)	N/A	jane doe	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.threats[]	Indicator.Attribute	Threat	N/A	N/A	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.subject	Indicator.Attribute	Email Subject	N/A	Your account has been compromised	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.friendlyName	Incident.Attribute	Affected Application	N/A	Microsoft SharePoint Online	Applicable if .value.entities[].properties.kind = 'CloudApplication'
.value.entities[].properties.recipient	Incident.Attribute	Recipient	N/A	N/A	Applicable if .value.entities[].properties.kind = 'MailMessage'
.value.entities[].properties.value	Malware.Value	N/A	N/A	N/A	Applicable if .value.entities[].properties.kind = 'Malware'
.value.entities[].properties.category	Malware.Attribute	Category	N/A	N/A	Applicable if .value.entities[].properties.kind = 'Malware'

Hash Type Mapping

AZURE SENTINEL ALGORITHM	THREATQ TYPE
MD5	MD5
SHA1	SHA-1
SHA256	SHA-256
SHA512	SHA-512

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.

Microsoft Azure Sentinel Incidents

METRIC	RESULT
Run Time	1 minute
Incidents	28
Incident Attributes	512
Indicators	31

Known Issues / Limitations

- The scope for authentication is `https://management.azure.com/.default` which means non-standard practices for authentication are required.

Change Log

- **Version 1.2.2**
  - Added support for Microsoft US Government Cloud environments.
  - Added the following new configuration parameters:
    - **Microsoft Azure Type** - allows you to select the Microsoft Azure Cloud environment. Options include `Microsoft Azure Global` and `Microsoft Azure US Government`.
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determines if the feed should honor proxy settings set in the ThreatQ UI.
- **Version 1.2.1**
  - Fixed an issue where users encountered a `KeyError` when they received a response that included an `Account` value without a corresponding `accountName` value.
- **Version 1.2.0**
  - Fixed an issue where users encountered an `Error creating objects from threat data` message when creating objects.
- **Version 1.1.0**
  - Fixed an issue where users encountered an `Error applying filter` message when using certain query ranges.
- **Version 1.0.0**
  - Initial Release