ThreatQuotient

ThreatQ CDF for Microsoft Defender

Version 1.3.0

March 17, 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	1.3.0
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQ CDF for Microsoft Defender integration enables the automatic ingestion of incidents, alerts, reports and related context, from your Microsoft Defender portal, into ThreatQ.

The integration provides the following endpoints:

- **Microsoft Defender XDR Incidents** - ingests incidents, alerts, and related context from Microsoft Defender.
- **Microsoft Defender Threat Intelligence Articles** - ingests reports, indicators, attack patterns and vulnerabilities.
- **Microsoft Defender Threat Intelligence Intel Profiles** - ingests adversaries, tools, reports and indicators.

The integration ingests the following system objects:

- Attack Patterns
- Assets
  - Asset Attributes
- Events
  - Event Attributes
- Indicators
  - Indicator Attributes
- Malware
- Reports
- Tags
- Tools
- Vulnerabilities

Prerequisites

The following is required to run the operation:

- A ThreatQ App registration in Microsoft Azure - see the following link for more information - https://learn.microsoft.com/en-us/azure/azure-monitor/logs/api/register-app-for-token.
- A Microsoft 365 Defender Tenant ID.
- A Microsoft 365 Defender Client ID.
- A Microsoft 365 Defender Client Secret.
- Your Azure Application must have Microsoft ThreatQ Protection permissions.
- Threat Intelligence feeds - an active Defender Threat Intelligence Portal license and Add-on.

Azure Application Threat Intelligence Permissions

Your Microsoft Azure Application must have **Microsoft Threat Protection** access for the `Incident.Read.All` permission for the **Microsoft 365 Defender Incidents** feed provided by this integration.

1. Select **Add a Permission** under the API permissions for your Azure Application.
2. Click on the **APIs my organization uses** tab.
3. Search for **Microsoft Threat Protection** and select the result.
4. Select the **Application Permissions** box when prompted.
5. Search and enable the `Incident.Read.All` permission.
6. Click the **Add permissions** button.
7. Click on **Grant admin consent for <Organization>** button to fully enable the permissions.

> This last step may take several minutes to propagate the permissions to your application.

Threat Intelligence Feeds

For **Threat Intelligence** feeds, your organization requires an active Defender Threat Intelligence Portal license and API add-on license for the tenant.

Additionally, your Microsoft Azure Application must have access for the `ThreatIntelligence.Read.All` permission.

1. On your application page, select `API Permissions` > `Microsoft Graph`.
2. In the page displayed, select `Application permissions`, start typing `ThreatIntelligence` in the search box, and select `ThreatIntelligence.Read.All` and then click on Add Permission.
3. Click `admin consent` for your tenant. You can select multiple permissions and then grant admin consent for them all.

More information about **Threat Intelligence** can be found here:

- https://techcommunity.microsoft.com/t5/microsoft-defender-threat/what-s-new-apis-in-microsoft-graph/ba-p/3780350

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the yaml 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 individual feeds to install, when prompted, and 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(s).

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:

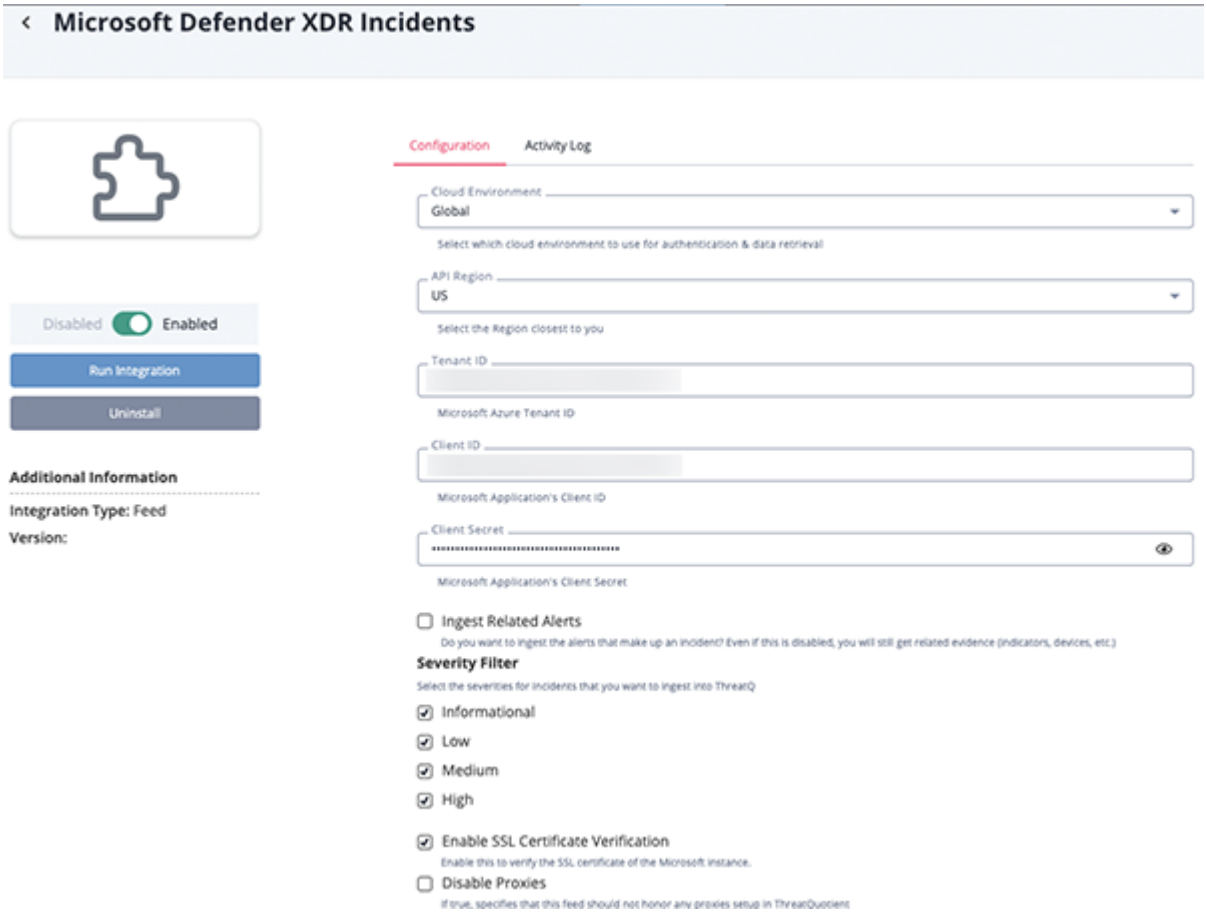
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

XDR Incidents Parameters

PARAMETER	DESCRIPTION
Cloud Environment	Select the cloud environment to use for authentication and data retrieval. Options include: ◦ Global (default) ◦ Government Community Cloud ◦ Government Community Cloud High & DoD
API Region	Select the region closest to your location. Options include: • US (Default) • EU • UK
Tenant ID	Your Microsoft Azure Tenant ID.
Client ID	Microsoft Application's Client ID.
Client Secret	Your Microsoft Application's Client Secret.
Ingest Related Alerts	Select whether to ingest the alerts that make up an incident. If this option is not selected, the integration will still ingest related evidence (indicators, devices, etc.).
Severity Filter	Select the severity of incidents to ingest into the ThreatQ Platform. Options include: ◦ Informational (default) ◦ Low (default) ◦ Medium (default) ◦ High (default)
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.

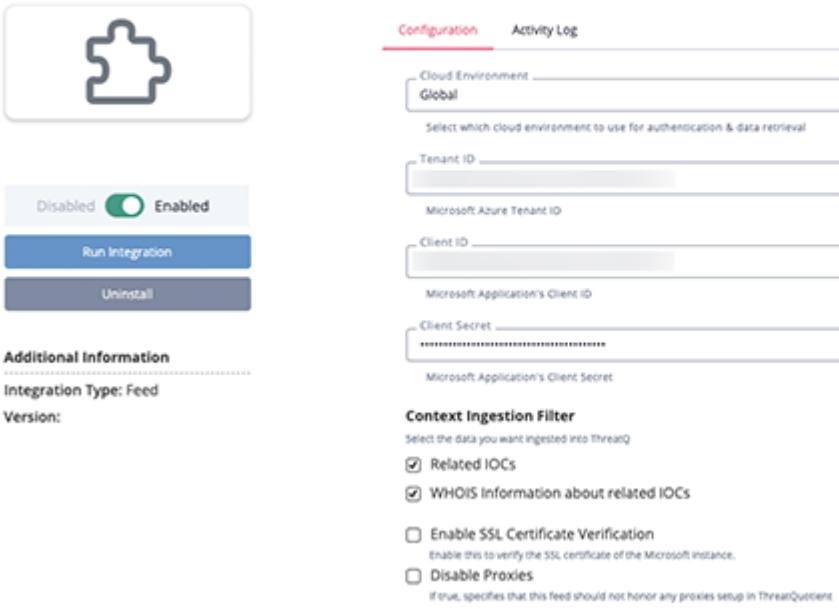


Threat Intelligence Intel Profiles Parameter

PARAMETER	DESCRIPTION
Cloud Environment	Select the cloud environment to use for authentication and data retrieval. Options include: ◦ Global (default) ◦ US Government L4 ◦ US Government L5 (DoD)
Tenant ID	Your Microsoft Azure Tenant ID.
Client ID	Microsoft Application's Client ID.
Client Secret	Your Microsoft Application's Client Secret.

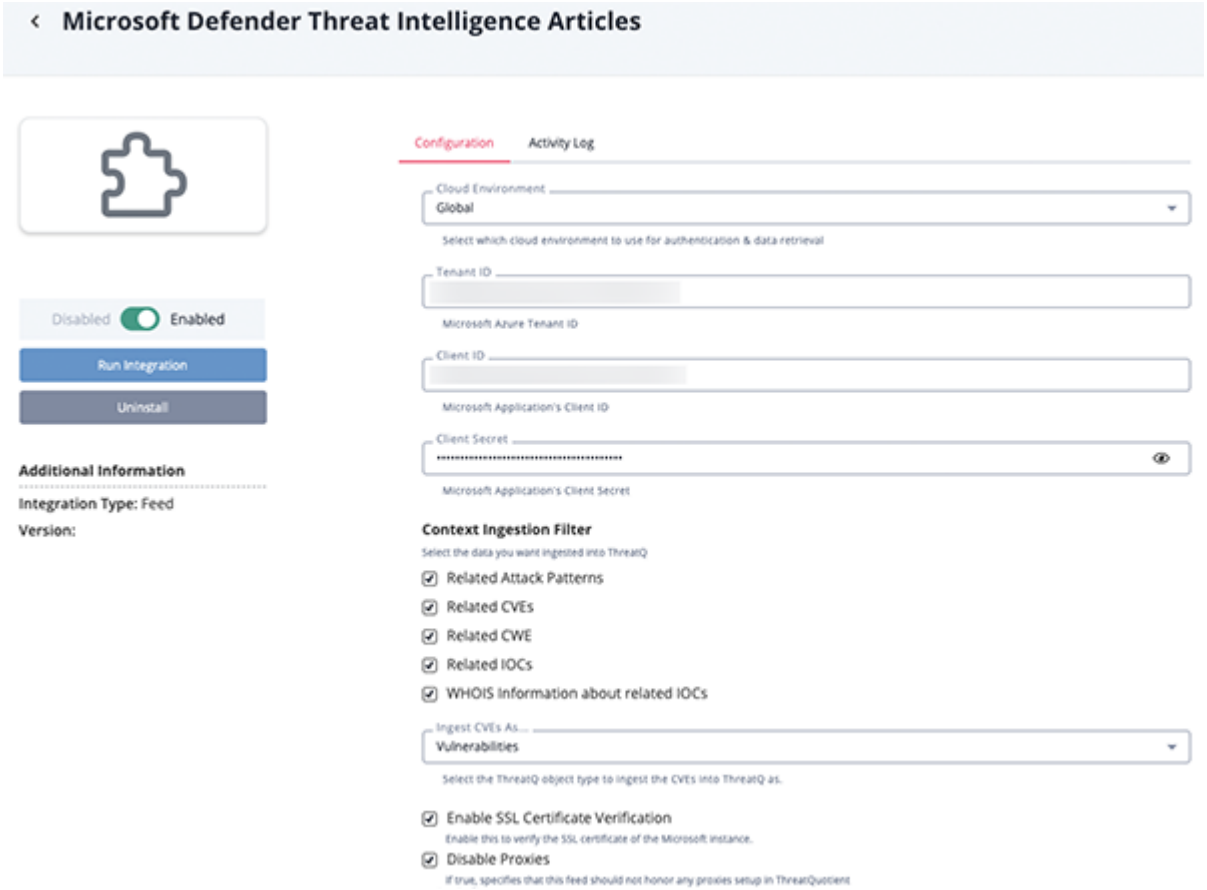
PARAMETER	DESCRIPTION
Context Ingestion Filter	Select the data you want ingested into ThreatQ. Options include: • Related IOCs • WHOIS Information about related IOCs
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

Microsoft Defender Threat Intelligence Intel Profiles



Threat Intelligence Articles Parameters

PARAMETER	DESCRIPTION
Cloud Environment	Select the cloud environment to use for authentication and data retrieval. Options include: ◦ Global (default) ◦ US Government L4 ◦ US Government L5 (DoD)
Tenant ID	Your Microsoft Azure Tenant ID.
Client ID	Microsoft Application's Client ID.
Client Secret	Your Microsoft Application's Client Secret.
Context Ingestion Filter	Select the data you want ingested into ThreatQ. Options include: • Related Attack Patterns • Related CVEs • Related CWE • Related IOCs • WHOIS Information about related IOCs
Ingest CVEs As	Select the ThreatQ object type to ingest the CVEs as into ThreatQ. Options include: ◦ Indicators ◦ Vulnerabilities (default)
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.



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 Defender XDR Incidents

The Microsoft Defender XDR Incidents feed automatically pulls incidents, alerts, and related context from Microsoft Defender.

Global - `GET https://<region>.security.microsoft.com/api/incidents?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

Government Community Cloud - `GET https://api-gcc.security.microsoft.us/api/incidents?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

Government Community Cloud High & DoD - `GET https://api-gov.security.microsoft.us/api/incidents?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

Sample Response:


```
{
    "@odata.context": "https://api.security.microsoft.com/api/
$metadata#Incidents",
    "value": [
        {
            "incidentId": 924521,
            "redirectIncidentId": null,
            "incidentName": "'Mimikatz' hacktool was detected on one endpoint",
            "createdTime": "2020-09-06T12:18:03.6266667Z",
            "lastUpdateTime": "2020-09-06T12:18:03.81Z",
            "assignedTo": null,
            "classification": "Unknown",
            "determination": "NotAvailable",
            "status": "Active",
            "severity": "Low",
            "tags": [],
            "comments": [],
            "alerts": [
                {
                    "alertId": "da637349914833441527_393341063",
                    "incidentId": 924521,
                    "serviceSource": "MicrosoftDefenderATP",
                    "creationTime": "2020-09-06T12:18:03.3285366Z",
                    "lastUpdatedTime": "2020-09-06T12:18:04.2566667Z",
                    "resolvedTime": null,
                    "firstActivity": "2020-09-06T12:15:07.7272048Z",
                    "lastActivity": "2020-09-06T12:15:07.7272048Z",
                    "title": "'Mimikatz' hacktool was detected",
```

```
                    "description": "Readily available tools, such as hacking
programs, can be used by unauthorized individuals to spy on users. When used by
attackers, these tools are often installed without authorization and used to
compromise targeted machines.\n\nThese tools are often used to collect personal
information from browser records, record key presses, access email and instant
messages, record voice and video conversations, and take screenshots.\n\nThis
detection might indicate that Windows Defender Antivirus has stopped the tool
from being installed and used effectively. However, it is prudent to check the
machine for the files and processes associated with the detected tool.",
                    "category": "Malware",
                    "status": "New",
                    "severity": "Low",
                    "investigationId": null,
                    "investigationState": "UnsupportedOs",
                    "classification": null,
                    "determination": null,
                    "detectionSource": "WindowsDefenderAv",
                    "assignedTo": null,
                    "actorName": null,
                    "threatFamilyName": "Mimikatz",
                    "mitreTechniques": [],
                    "devices": [
                        {
                            "mdatpDeviceId":
"24c222b0b60fe148eeece49ac83910cc6a7ef491",
                            "aadDeviceId": null,
                            "deviceDnsName":
"user5cx.middleeast.corp.contoso.com",
                            "osPlatform": "WindowsServer2016",
                            "version": "1607",
                            "osProcessor": "x64",
                            "osBuild": 14393,
                            "healthStatus": "Active",
                            "riskScore": "High",
                            "rbacGroupName": "WDATP-Ring0",
                            "rbacGroupId": 9,
                            "firstSeen": "2020-02-06T14:16:01.9330135Z"
                        }
                    ],
                    "entities": [
                        {
                            "entityType": "File",
                            "sha1": "5de839186691aa96ee2ca6d74f0a38fb8d1bd6dd",
                            "sha256": null,
                            "fileName": "Detector.UnitTests.dll",
                            "filePath": "C:\\Agent\\_work\\_temp\\Deploy_SYSTEM
2020-09-06 12_14_54\\Out",
                            "processId": null,
                            "processCommandLine": null,
                            "processCreationTime": null,
```

```
                            "parentProcessId": null,
                            "parentProcessCreationTime": null,
                            "ipAddress": null,
                            "url": null,
                            "accountName": null,
                            "domainName": null,
                            "userSid": null,
                            "aadUserId": null,
                            "userPrincipalName": null,
                            "mailboxDisplayName": null,
                            "mailboxAddress": null,
                            "clusterBy": null,
                            "sender": null,
                            "recipient": null,
                            "subject": null,
                            "deliveryAction": null,
                            "securityGroupId": null,
                            "securityGroupName": null,
                            "registryHive": null,
                            "registryKey": null,
                            "registryValueType": null,
                            "registryValue": null,
                            "deviceId":
"24c222b0b60fe148eeece49ac83910cc6a7ef491"
                        }
                    ]
                }
            ]
        }
    ]
}
```


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[].[incidentName/severity]`	Event.Title	Incident	`.value[].alerts[].createdTime`	`<incident name> [<severity>]`	Keys are concatenated to form title
`.value[].alerts[].firstActivity`	Event.Happened_at	N/A	N/A	2020-09-06T12:18:03.3285366Z	N/A
`.value[].alerts[].[x]`	Event.Description	N/A	N/A	N/A	This field will be HTML, a description is built from asset context
`.value[].tags[]`	Event.Tag	N/A	N/A	N/A	N/A
`.value[].classification`	Event.Attribute	Classification	`.value[].alerts[].createdTime`	False Positive	Mapped to a more human-readable value

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value[].incidentUri`	Event.Attribute	Incident Link	`.value[].alerts[].createdTime`	N/A	N/A
`.value[].incidentId`	Event.Attribute	Incident ID	`.value[].alerts[].createdTime`	4	N/A
`.value[].severity`	Event.Attribute	Severity	`.value[].alerts[].createdTime`	High	N/A
`.value[].status`	Event.Attribute	Status	`.value[].alerts[].createdTime`	Open	N/A
`.value[].determination`	Event.Attribute	Determination	`.value[].alerts[].createdTime`	Unwanted Software	Mapped to a more human-readable value
`.value[].comments[].comment`	Event.Attribute	Comment	`.value[].alerts[].createdTime`	N/A	N/A
`.value[].detectionSource`	Event.Attribute	Detection Source	`.value[].alerts[].createdTime`	Microsoft Defender ATP	Mapped to a more human-readable value
`.value[].assignedTo`	Event.Attribute	Assigned To	`.value[].alerts[].createdTime`	N/A	N/A
`.value[].alerts[].title`	Event Title	N/A	`.alerts[].CreationTime`	N/A	N/A
`.value[].alerts[].description`	Description	N/A	N/A	N/A	N/A
`.value[].alerts[].mitreTechniques`	Attack Pattern.Value	N/A	`.alerts[].CreationTime`	N/A	N/A
`.value[].alerts[].threatFamilyName`	Malware.Value	N/A	`.alerts[].CreationTime`	N/A	N/A
`.value[].alerts[].actorName`	Adversary.Value	N/A	`.alerts[].CreationTime`	N/A	N/A
`.value[].alerts[].serviceSource`	Event.Attribute	Service Source	`.alerts[].CreationTime`	Office ATP	Mapped to a more human-readable value
`.value[].alerts[].category`	Event.Attribute	Tactic	`.alerts[].CreationTime`	Initial Access	Mapped to a more human-readable value
`.value[].alerts[].status`	Event.Attribute	Status	`.alerts[].CreationTime`	New	Mapped to a more human-readable value

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value[].alerts[].severity`	Event.Attribute	Severity	`.alerts[].CreationTime`	Medium	Mapped to a more human-readable value
`.value[].alerts[].investigationState`	Event.Attribute	Investigation State	`.alerts[].CreationTime`	Successfully Remediated	Mapped to a more human-readable value
`.value[].alerts[].classification`	Event.Attribute	Classification	`.alerts[].CreationTime`	Not set	Mapped to a more human-readable value
`.value[].alerts[].determination`	Event.Attribute	Determination	`.alerts[].CreationTime`	Not set	Mapped to a more human-readable value
`.value[].alerts[].detectionSource`	Event.Attribute	Tactic	`.alerts[].CreationTime`	Microsoft Defender ATP	Mapped to a more human-readable value
`.value[].alerts[].entities[].sha1`	Indicator.Value	SHA-1	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].sha256`	Indicator.Value	SHA-256	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].fileName`	Indicator.Value	Filename	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].filePath`	Indicator.Value	File Path	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].ipAddress`	Indicator.Value	IP Address	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Active
`.value[].alerts[].entities[].url`	Indicator.Value	FQDN or URL	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Active, type changes based on content
`.value[].alerts[].entities[].mailboxAddress`	Indicator.Value	Email Address	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].mailboxDisplayName`	Indicator.Attribute	Display Name	`.alerts[].entities[].evidenceCreationTime`	N/A	Only added to Email indicator
`.value[].alerts[].entities[].sender`	Indicator.Value	Email Address	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value[].alerts[].entities[].userPrincipalName`	Indicator.Value	Email Address	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].accountName`	Indicator.Value	Username	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].subject`	Indicator.Value	Email Subject	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].registryKey`	Indicator.Value	Registry Key	`.alerts[].entities[].evidenceCreationTime`	N/A	Defaults Status: Review
`.value[].alerts[].entities[].verdict`	Indicator.Attribute	Verdict	`.alerts[].entities[].evidenceCreationTime`	N/A	N/A
`.value[].alerts[].entities[].detectionStatus`	Indicator.Attribute	Detection Status	`.alerts[].entities[].evidenceCreationTime`	Healthy	N/A
`.value[].alerts[].devices[].deviceDnsName`	Asset.Value	N/A	`.alerts[].devices[].firstSeen`	user5cx.middleeast.corp.contoso.com	N/A
`.value[].alerts[].devices[].deviceDnsName`	Asset.Attribute	Hostname	`.alerts[].devices[].firstSeen`	user5cx.middleeast.corp.contoso.com	N/A
`.value[].alerts[].devices[].osPlatform`	Asset.Attribute	Operating System	`.alerts[].devices[].firstSeen`	Windows Server 2016	Replaces some values to make it more human-readable
`.value[].alerts[].devices[].healthStatus`	Asset.Attribute	Health Status	`.alerts[].devices[].firstSeen`	Healthy	N/A
`.value[].alerts[].devices[].riskScore`	Asset.Attribute	Risk Score	`.alerts[].devices[].firstSeen`	N/A	N/A
`.value[].alerts[].devices[].rbacGroupName`	Asset.Attribute	RBAC Group	`.alerts[].devices[].firstSeen`	N/A	N/A
`.value[].alerts[].devices[].defenderAvStatus`	Asset.Attribute	AV Status	`.alerts[].devices[].firstSeen`	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value[].alerts[].devices[].onboardingStatus`	Asset.Attribute	Onboarding Status	`.alerts[].devices[].firstSeen`	N/A	N/A
`.value[].alerts[].devices[].tags`	Asset.Tag	N/A	N/A	N/A	N/A

Microsoft Defender Threat Intelligence Articles

The Microsoft Defender Threat Intelligence Articles feed pulls articles and related context from Microsoft Threat Intelligence.

Global - `GET https://graph.microsoft.com/v1.0/security/threatIntelligence/articles?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

US Government L4 - `GET https://graph.microsoft.us/v1.0/security/threatIntelligence/articles?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

US Government L5 (DoD) - `GET https://dod-graph.microsoft.us/v1.0/security/threatIntelligence/articles?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

Sample Response:


```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#security/threatIntelligence/articles",
  "@odata.nextLink": "https://graph.microsoft.com/v1.0/security/threatIntelligence/articles?$skip=25",
  "value": [
    {
      "id": "2f8526bf",
      "createdDateTime": "2023-11-07T21:33:55.553Z",
      "lastUpdatedDateTime": "2023-11-07T21:33:55.553Z",
      "title": "Unmasking AsyncRAT New Infection Chain",
      "isFeatured": false,
      "tags": [
        "OSINT",
        "AsyncRAT",
        "Phishing",
        "T1566 - Phishing",
        "T1064 - Scripting",
        "T1056 - Input Capture",
        "T1055 - Process Injection",
        "T1082 - System Information Discovery",
        "T1057 - Process Discovery",
        "T1083 - File and Directory Discovery",
        "TA0008 - Lateral Movement",
        "CVE-2023-3519",
        "CWE-20 - Improper Input Validation"
      ],
      "imageUrl": null,
      "summary": {
        "content": "McAfee Labs has observed a recent AsyncRAT campaign being distributed through a malicious HTML file. This entire infection strategy employs a range of file types, including PowerShell, Windows Script File (WSF),
```

```
VBScript (VBS), and more, in order to bypass antivirus detection measures.",
        "format": "markdown"
      },
      "body": {
        "content": "#### Description\r\nMcAfee Labs has observed a recent
AsyncRAT campaign being distributed through a malicious HTML file. This entire
infection strategy employs a range of file types, including PowerShell, Windows
Script File (WSF), VBScript (VBS), and more, in order to bypass antivirus
detection measures.",
        "format": "markdown"
      }
    }
  ]
}
```

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[].title`	Report.Value	N/A	`.value[].createdDateTime`	`Microsoft Threat Intelligence: Unmasking AsyncRAT New Infection Chain`	Prepended with `Microsoft Threat Intelligence:`
`.value[].summary.content`, `.value[].body.content`	Report.Description	N/A	N/A	`Summary .value[].summary.content Body .value[].body.content`	Values are concatenated
`.value[].tags`	Report.Tags	N/A	N/A	`OSINT`	If the value is not attack pattern, CVE or CWE.
`.value[].tags`	Related Attack Pattern.Value	N/A	`.value[].createdDateTime`	`T1566 - Phishing`	If the value respects Mitre Att&CK naming convention and `Related Attack Patterns` is enabled
`.value[].tags`	Related Indicator/ Vulnerability.Value	N/A	`.value[].createdDateTime`	`CVE-2023-3519`	If the value starts with `CVE`. Ingestion depends on `Ingest CVEs As...` user config. If `Related CVEs` is enabled
`.value[].tags`	Related Vulnerability.Value	N/A	`.value[].createdDateTime`	`CWE-20 - Improper Input Validation`	If the value starts with `CWE` and `Related CWE` is enabled

Microsoft Defender Threat Intelligence Intel Profiles

The Microsoft Defender Threat Intelligence Intel Profiles feed provides up-to-date threat actor infrastructure visibility.

Global - `GET https://graph.microsoft.com/v1.0/security/threatIntelligence/intelProfiles?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

US Government L4 - `GET https://graph.microsoft.us/v1.0/security/threatIntelligence/intelProfiles?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

US Government L5 (DoD) - `GET https://dod-graph.microsoft.us/v1.0/security/threatIntelligence/intelProfiles?$filter="lastUpdateTime ge {{since}} and lastUpdateTime le {{until}}"&$skip=0&$top=100`

Sample Response:


```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#security/threatIntelligence/intelProfiles",
  "value": [
    {
      "id": "eb747f064dc5702e50e28b63e4c74ae2e6ae19ad7de416902e998677b4ad72ff",
      "kind": "tool",
      "title": "Akira ransomware",
      "firstActiveDateTime": "2023-06-27T00:00:00Z",
      "aliases": [],
      "targets": [],
      "tradecraft": null,
      "summary": {
        "content": "Akira is a new\nransomware strain first observed by Microsoft Threat Intelligence in March 2023.",
        "format": "markdown"
      },
      "description": {
        "content": "## Snapshot\r\nAkira is a new ransomware strain first observed by Microsoft Threat Intelligence in March 2023.",
        "format": "markdown"
      },
      "countriesOrRegionsOfOrigin": []
    },
    {
      "id": "663a34023b3cf75910339e90c73d78a7cb18b8c0c7be260f63902c5a6d306d5b",
      "kind": "actor",
      "title": "Blue Tsunami",
      "firstActiveDateTime": "2022-01-01T00:00:00Z",
      "aliases": [
        "Blue"
      ],
```

```
      "targets": [
        "Financial Services",
        "Non-Government Organization",
        "Other business entities"
      ],
      "summary": {
        "content": "The actor Microsoft tracks as Blue Tsunami is a private
sector offensive actor (PSOA) group based out of Israel.",
        "format": "markdown"
      },
      "description": {
        "content": "## Snapshot\r\nThe actor Microsoft tracks as Blue Tsunami
is a private sector offensive actor (PSOA) group based out of Israel.",
        "format": "markdown"
      },
      "tradecraft": {
        "content": "Blue Tsunami leverages Microsoft and LinkedIn resources by
creating fake personas to lure targets.",
        "format": "markdown"
      },
      "countriesOrRegionsOfOrigin": [
        {
          "label": "Israel",
          "code": "il"
        }
      ]
    }
  ]
}
```


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[].title`	Adversary/Tool/ Report.Value	N/A	`.value[].firstActiveDateTime`	`Akira ransomware`	Mapping done according to `Microsoft Intel Profile Mapping` using `.value[].kind`
`.value[].summary.content`, `.value[].description.content`, `.value[].tradecraft.content`	Adversary/Tool/ Report.Description	N/A	N/A	`Summary .value[].summary.content Description .value[].description.content Tradecraft .value[].tradecraft.content`	Values are concatenated
`.value[].countriesOrRegionsOfOrigin[].label`	Adversary/Tool/ Report.Attribute	Country	`.value[].firstActiveDateTime`	`Israel`	N/A
`.value[].countriesOrRegionsOfOrigin[].code`	Adversary/Tool/ Report.Attribute	Country Code	`.value[].firstActiveDateTime`	`IL`	All-uppercase.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value[].countriesOrRegionsOfOrigin[].targets`	Adversary/Tool/ Report.Attribute	Target	`.value[].firstActiveDateTime`	`Financial Services`	N/A
`.value[].countriesOrRegionsOfOrigin[].aliases`	Adversary/Tool/ Report.Attribute	Alias	`.value[].firstActiveDateTime`	`Blue`	N/A

Microsoft Intel Profile Mapping

The following mapping table display the Microsoft Unclassified Artifact to ThreatQ object type mapping.

MICROSOFT UNCLASSIFIED ARTIFACT KIND	THREATQ OBJECT TYPE
actor	Adversary
tool	Tool
unknownFutureValue	Report

Microsoft Defender Threat Intelligence Indicators (supplemental)

The Intelligence Indicators supplemental feed will ingests related Indicators of compromise if you have selected the `Related IOCs` option selected under the **Context Ingestion Filter** for the Microsoft Defender Threat Intelligence Intel Profiles and Articles feeds.

Articles

Global - `GET https://graph.microsoft.com/v1.0/security/threatIntelligence/articles/{{ARTICLE_ID}}/indicators`

US Government L4 - `GET GET https://graph.microsoft.us/v1.0/security/threatIntelligence/articles/{{ARTICLE_ID}}/indicators`

US Government L5 (DoD) - `GET GET https://dod-graph.microsoft.us/v1.0/security/threatIntelligence/articles/{{ARTICLE_ID}}/indicators`

Intel Profiles

Global - `GET https://graph.microsoft.com/v1.0/security/threatIntelligence/intelProfiles/{{PROFILE_ID}}/indicators`

US Government L4 - `GET https://graph.microsoft.us/v1.0/security/threatIntelligence/intelProfiles/{{PROFILE_ID}}/indicators`

US Government L5 (DoD) - `GET https://dod-graph.microsoft.us/v1.0/security/threatIntelligence/intelProfiles/{{PROFILE_ID}}/indicators`

Sample Response:


```
{
  "value": [
    {
      "id":
"aGFzaF9zaGEyNTYkJDMyMzIyNmQ2ZjljOTVmZGEzZDc0NWE5YmNlMWVjZDZiNTM4YjQzNTFhYTFjNm
ZkYTA1NDkzODhlZWM1ODVkNjMkJHJpc2tpcQ==",
      "source": "microsoft",
      "firstSeenDateTime": "2021-07-15T23:35:10Z",
      "lastSeenDateTime": "2023-10-24T19:03:39.127Z",
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id":
"323226d6f9c95fda3d745a9bce1ecd6b538b4351aa1c6fda0549388eec585d63",
        "kind": "hash_sha256",
        "value":
"323226d6f9c95fda3d745a9bce1ecd6b538b4351aa1c6fda0549388eec585d63"
      }
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id": "609a925fd253e82c80262bad31637f19",
        "kind": "hash_md5",
        "value": "609a925fd253e82c80262bad31637f19"
      },
```

```
      "id":
"aGFzaF9tZDUkJDYwOWE5MjVmZDI1M2U4MmM4MDI2MmJhZDMxNjM3ZjE5JCRwdWJsaWM=",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id": "2d1ce0231cf8ff967c36bbfc931f3807ddba765c",
        "kind": "hash_sha1",
        "value": "2d1ce0231cf8ff967c36bbfc931f3807ddba765c"
      },
      "id":
"aGFzaF9zaGExJCQyZDFjZTAyMzFjZjhmZjk2N2MzNmJiZmM5MzFmMzgwN2RkYmE3NjVjJCRwdWJsaW
M=",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id": "keishagrey994@outlook.com",
        "kind": "email",
        "value": "keishagrey994@outlook.com"
      },
      "id": "ZW1haWwkJGtlaXNoYWdyZXk5OTRAb3V0bG9vay5jb20kJHB1YmxpYw==",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id": "http://45.148.120.23:91/vmtools.exe",
        "kind": "url",
        "value": "http://45.148.120.23:91/vmtools.exe"
      },
      "id": "dXJsJCRodHRwOi8vNDUuMTQ4LjEyMC4yMzo5MS92bXRvb2xzLmV4ZSQkcHVibGlj",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id": "185.156.72.8:9890",
        "kind": "ip_port",
        "value": "185.156.72.8:9890"
      },
      "id": "aXBfcG9ydCQkMTg1LjE1Ni43Mi44Ojk4OTAkJHB1YmxpYw==",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.ipAddress",
        "id": "85.187.128.19"
```

```
      },
      "id": "aXAkJDg1LjE4Ny4xMjguMTkkJHB1YmxpYw==",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "roxylvfuco.com.au"
      },
      "id": "ZG9tYWluJCRyb3h5bHZmdWNvLmNvbS5hdSQkcmlza2lx",
      "source": "microsoft"
    }
  ]
}
```


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[].artifact.value`	Indicator.Value	`.value[].artifact.kind`	`.value[].firstSeenDateTime`	`323226d6f9c95fda3d7` `45a9bce1ecd6b538b4351aa1c6fda0549388eec585d63`	If `value[].artifact.@dataType` is `#microsoft.graph.security.unclassifiedArtifact` the mapping is done according to `Microsoft Unclassified Artifacts mapping`
`.value[].artifact.id`	Indicator.Value	`.value[].artifact.@data.type`	`.value[].firstSeenDateTime`	`85.187.128.19`	If `value[].artifact.@dataType` is not `#microsoft.graph.security.unclassifiedArtifact` the mapping is done according to `Microsoft Classified Artifact Types`
`.value[].artifact.source`	Indicator.Attribute	Source	N/A	`microsoft`	N/A

Microsoft Unclassified Artifacts Mapping

ThreatQuotient provides the following Unclassified Artifact Kind to ThreatQ Indicator Type mapping.

MICROSOFT UNCLASSIFIED ARTIFACT KIND	THREATQ INDICATOR TYPE
hash_sha256	SHA-256
hash_sha1	SHA-1
certificate_sha1	SHA-1
hash_md5	MD5
url	URL
email	Email Address

Microsoft Classified Artifacts Mapping

ThreatQuotient provides the following Classified Artifact Kind to ThreatQ Indicator Type mapping.

MICROSOFT CLASSIFIED ARTIFACT KIND	THREATQ INDICATOR TYPE
#microsoft.graph.security.hostname	FQDN
#microsoft.graph.security.ipAddress	IP Address/IPv6 Address

Microsoft Defender Threat Intelligence Host WHOIS (supplemental)

The Threat Intelligence Host WHOIS supplemental feed will ingests WHOIS information about indicators of type FQDN and IP Addresses if you have selected the `WHOIS Information about related IOCs` option selected under the **Context Ingestion Filter** for the Microsoft Defender Threat Intelligence Intel Profiles and Articles feeds.

Global - `GET https://graph.microsoft.com/v1.0/security/threatIntelligence/hosts/{{HOST_ID}}/whois`

US Government L4 - `GET https://graph.microsoft.us/v1.0/security/threatIntelligence/hosts/{{HOST_ID}}/whois`

US Government L5 (DoD) - `GET https://dod-graph.microsoft.us/v1.0/security/threatIntelligence/hosts/{{HOST_ID}}/whois`

Sample Response:


```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#microsoft.graph.security.whoisRecord",
  "id": "cm94eWx2ZnVjby5jb20uYXUkJDcxMTA4OTI3NzQzODM4NDQ2MTA=",
  "expirationDateTime": null,
  "registrationDateTime": "2023-06-22T00:52:33Z",
  "firstSeenDateTime": null,
  "lastSeenDateTime": null,
  "lastUpdateDateTime": "2023-10-24T11:06:15.164Z",
  "abuse": null,
  "admin": null,
  "billing": null,
  "registrar": null,
  "noc": null,
  "zone": null,
  "whoisServer": "whois.auda.org.au",
  "domainStatus": "serverRenewProhibited https://identitydigital.au/get-au/
whois-status-codes#serverRenewProhibited",
  "rawWhoisText": "Domain Name: ROXYLVFUCO.COM.AU\nRegistry Domain ID:
D407400000135091064-AU\nRegistrar WHOIS Server: whois.auda.org.au\nRegistrar
URL: https://www.instra.com/en/about-us/contact-us\nLast Modified:
2023-06-22T00:52:33Z\nRegistrar Name: Domain Directors Pty Ltd trading as
Instra\nRegistrar Abuse Contact Email: abuse@key-systems.net\nRegistrar Abuse
Contact Phone: +49.68949396850\nReseller Name:\nStatus: serverRenewProhibited
https://identitydigital.au/get-au/whois-status-
codes#serverRenewProhibited\nStatus Reason: Not Currently Eligible For
Renewal\nRegistrant Contact ID: EST2724909620\nRegistrant Contact Name: Ejay
Turner\nTech Contact ID: EST2724909620\nTech Contact Name: Ejay Turner\nName
Server: ASHLEY.NS.CLOUDFLARE.COM\nName Server:
EUGENE.NS.CLOUDFLARE.COM\nDNSSEC: unsigned\nRegistrant: PERPETUAL TRUSTEE
COMPANY LIMITED\nRegistrant ID: ACN 000001007\nEligibility Type: Other\n\n>>>
Last update of WHOIS database: 2023-09-22T07:49:00Z <<<\n\n\n\nIdentity Digital
Australia Pty Ltd (Identity Digital), for itself and on behalf of .au Domain
Administration Limited (auDA), makes the WHOIS registration data directory
```

```
service (WHOIS Service) available solely for the purposes of:\n\n(a) querying
the availability of a domain name licence;\n\n(b) identifying the holder of a
domain name licence; and/or\n\n(c) contacting the holder of a domain name
licence in relation to that domain name and its use.\n\nThe WHOIS Service must
not be used for any other purpose (even if that purpose is lawful), including:
\n\n(a) aggregating, collecting or compiling information from the WHOIS
database, whether for personal or commercial purposes;\n\n(b) enabling the
sending of unsolicited electronic communications; and / or\n\n(c) enabling high
volume, automated, electronic processes that send queries or data to the
systems of Identity Digital, any registrar, any domain name licence holder, or
auDA.\n\nThe WHOIS Service is provided for information purposes only. By using
the WHOIS Service, you agree to be bound by these terms and conditions. The
WHOIS Service is operated in accordance with the auDA WHOIS Policy (available
at https://www.auda.org.au/policies/index-of-published-policies/
2014/2014-07/ ).",
  "registrant": {
    "email": "abuse@key-systems.net",
    "name": "Ejay Turner",
    "organization": "PERPETUAL TRUSTEE COMPANY LIMITED",
    "telephone": null,
    "fax": null,
    "address": {
      "city": "sofia",
      "countryOrRegion": "bulgaria",
      "postalCode": "1756",
      "state": null,
      "street": "kambanite green offices 9 vitoshki kambani street,fl. 3"
    }
  },
  "technical": {
    "email": null,
    "name": "Ejay Turner",
    "organization": null,
    "telephone": null,
    "fax": null,
    "address": {
      "city": "sofia",
      "countryOrRegion": "bulgaria",
      "postalCode": null,
      "state": null,
      "street": "26a andrej saharov blvd."
    }
  },
  "nameservers": [
  ],
  "host": {
    "@odata.type": "#microsoft.graph.security.hostname",
    "id": "roxylvfuco.com.au"
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.registrationDateTime`	Indicator.Attribute	Registration Date	`.registrationDateTime`	`2023-06-22T00:52:33Z`	N/A
`.lastUpdateDateTime`	Indicator.Attribute	WHOIS Last Update	`.registrationDateTime`	`2023-10-24T11:06:15.164Z`	Updated if already exists
`.whoisServer`	Indicator.Attribute	WHOIS Server	`.registrationDateTime`	`whois.auda.org.au`	N/A
`.domainStatus`	Indicator.Attribute	Domain Status	`.registrationDateTime`	`serverRenewProhibited...`	Updated if already exists
`.registrant.email`	Indicator.Attribute	Registrant Email	`.registrationDateTime`	`abuse@key-systems.net`	N/A
`.registrant.name`	Indicator.Attribute	Registrant Name	`.registrationDateTime`	`Ejay Turner`	N/A
`.registrant.organization`	Indicator.Attribute	Registrant Organization	`.registrationDateTime`	`PERPETUAL TRUSTEE COMPANY LIMITED`	N/A
`.registrant.address.city`	Indicator.Attribute	Registrant City	`.registrationDateTime`	`Sofia`	Title cased
`.registrant.address.countryOrRegion`	Indicator.Attribute	Registrant Country	`.registrationDateTime`	`Bulgaria`	Title cased
`.registrant.address.postalCode`	Indicator.Attribute	Registrant Postal Code	`.registrationDateTime`	N/A	N/A
`.registrant.address.state`	Indicator.Attribute	Registrant State	`.registrationDateTime`	N/A	N/A
`.registrant.address.street`	Indicator.Attribute	Registrant Street	`.registrationDateTime`	`26a andrej saharov blvd.`	N/A

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 Defender XDR Incidents

METRIC	RESULT
Run Time	1 minute
Asset	1
Asset Attributes	5
Events	6
Event Attributes	37
Indicators	10
Indicator Attributes	2
Malware	1

Microsoft Defender Threat Intelligence Articles

METRIC	RESULT
Run Time	1 minute
Attack Pattern	44
Indicators	224
Indicator Attributes	226
Report	11
Vulnerability	1

Microsoft Defender Threat Intelligence Intel Profiles

METRIC	RESULT
Run Time	8 minutes
Adversaries	194
Adversary Attributes	906
Indicators	2431
Indicator Attributes	2477
Tool	64
Tool Attributes	4

Known Issues / Limitations

- When **Related IOCs** option is used the API may respond with a `HTTP 400` status error while fetching related indicators for the **Microsoft Defender Threat Intelligence Articles** and **Microsoft Defender Threat Intelligence Intel Profiles** feeds.

Change Log

- **Version 1.3.0**
  - Added support for Gov-Cloud and DoD environments.
  - Added the following new configuration parameters:
    - **Cloud Environment** - allows you to select the cloud environment.
    - **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.
  - Resolved a data parsing issue that would occur when the first seen date is missing for an asset.
  - Renamed the integration and provided feeds to reflect current vendor branding:
    - **ThreatQ CDF for Microsoft 365 Defender Incidents** is now **ThreatQ CDF for Microsoft Defender Incidents**.
      - **Microsoft 365 Defender Incidents** is now **Microsoft Defender XDR Incidents**.
      - **Microsoft 365 Defender Threat Intelligence Articles** is now **Microsoft Defender Threat Intelligence Articles**.
      - **Microsoft 365 Defender Threat Intelligence Intel Profiles** is now **Microsoft Defender Threat Intelligence Intel Profiles**.
- **Version 1.2.2 rev-a**
  - Guide Update - updated the requirements and permission sections in the **Prerequisites** chapter.
- **Version 1.2.2**
  - Fixed `FilterMapping` error for alert descriptions for Defender Incidents.
- **Version 1.2.1**
  - Resolved a `TypeError 'Cannot parse argument of type None'` error that would occur when the `.firstActivity` is missing for the Microsoft Incident.
- **Version 1.2.0**
  - Updated the integration name to Microsoft 365 Defender CDF.
  - Added two new feeds:
    - Microsoft 365 Defender Threat Intelligence Intel Profiles
    - Microsoft 365 Defender Threat Intelligence Articles
  - Added Known Issues / Limitations chapter to the user guide.
  - Updated the Prerequisites chapter of the user guide.
  - Updated the minimum ThreatQ version to 5.10.0
- **Version 1.1.1**
  - Fixed a `FilterMapping` error that occurred with Alert descriptions.
- **Version 1.1.0 rev-a (Guide Update)**
  - Updated the Prerequisites chapter regarding the Asset object. ThreatQ version 5.10.0 introduced the Asset object as a seeded default system object. Users on ThreatQ 5.10.0 or later do not have to install the Asset custom object prior to installing the integration.
- **Version 1.1.0**

  - Fixed an object ingestion error caused when trying to deduplicate dictionaries.
  - Fixed a timestamp issue.
  - Uploaded custom object installation steps.
- **Version 1.0.0**
  - Initial release