

# ThreatQuotient



## ThreatQ CDF for Microsoft 365 Defender

Version 1.2.1

May 13, 2024

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

### Support

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

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

Phone: 703.574.9893

# Contents

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>Warning and Disclaimer .....</b>                                       | <b>3</b>  |
| <b>Support .....</b>                                                      | <b>4</b>  |
| <b>Integration Details.....</b>                                           | <b>5</b>  |
| <b>Introduction .....</b>                                                 | <b>6</b>  |
| <b>Prerequisites .....</b>                                                | <b>7</b>  |
| Microsoft Azure Application Access .....                                  | 7         |
| Threat Intelligence Feeds.....                                            | 7         |
| <b>Installation .....</b>                                                 | <b>8</b>  |
| <b>Configuration .....</b>                                                | <b>9</b>  |
| All Feeds .....                                                           | 9         |
| Incidents - Additional Parameters .....                                   | 10        |
| Threat Intelligence Intel Profiles - Additional Parameter .....           | 10        |
| Threat Intelligence Articles - Additional Parameters .....                | 11        |
| <b>ThreatQ Mapping.....</b>                                               | <b>12</b> |
| Microsoft 365 Defender Incidents (Feed).....                              | 12        |
| Microsoft 365 Defender Threat Intelligence Articles .....                 | 18        |
| Microsoft 365 Defender Threat Intelligence Intel Profiles .....           | 20        |
| Microsoft Intel Profile Mapping.....                                      | 22        |
| Microsoft 365 Defender Threat Intelligence Indicators (supplemental)..... | 23        |
| Microsoft Unclassified Artifacts Mapping .....                            | 26        |
| Microsoft Classified Artifacts Mapping.....                               | 27        |
| Microsoft 365 Defender Threat Intelligence Host WHOIS (supplemental)..... | 28        |
| <b>Average Feed Run.....</b>                                              | <b>31</b> |
| Microsoft 365 Defender Incidents .....                                    | 31        |
| Microsoft 365 Defender Threat Intelligence Articles .....                 | 32        |
| Microsoft 365 Defender Threat Intelligence Intel Profiles .....           | 33        |
| <b>Known Issues / Limitations .....</b>                                   | <b>34</b> |
| <b>Change Log .....</b>                                                   | <b>35</b> |

# Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2024 ThreatQuotient, Inc.

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

# Support

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

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

**Support Web:** <https://support.threatq.com>

**Support Phone:** 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

# Integration Details

ThreatQuotient provides the following details for this integration:

|                                  |                   |
|----------------------------------|-------------------|
| Current Integration Version      | 1.2.1             |
| Compatible with ThreatQ Versions | >= 5.10.0         |
| Support Tier                     | ThreatQ Supported |

# Introduction

The ThreatQ CDF for Microsoft 365 Defender integration enables the automatic ingestion of incidents, alerts, reports and related context, from your Microsoft 365 Defender portal, into ThreatQ.

The integration provides the following endpoints:

- **Microsoft 365 Defender Incidents** - ingests incidents, alerts, and related context from Microsoft 365 Defender.
- **Microsoft 365 Defender Threat Intelligence Articles** - ingests reports, indicators, attack patterns and vulnerabilities.
- **Microsoft 365 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

Review the following prerequisites before attempting to install the Microsoft 365 Defender Incidents CDF integration.

## Microsoft Azure Application Access

Your Microsoft Azure Application must have `Application` access for the `Incident.Read.All` permission.

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



This last step may take a few 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



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.

6. If prompted, select the individual feeds to install and click **Install**. The feed 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 **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:

## All Feeds

| PARAMETER     | DESCRIPTION                                 |
|---------------|---------------------------------------------|
| Tenant ID     | Your Microsoft Azure Tenant ID.             |
| Client ID     | Microsoft Application's Client ID.          |
| Client Secret | Your Microsoft Application's Client Secret. |

## Incidents - Additional Parameters

| PARAMETER             | DESCRIPTION                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| API Region            | Select the region closest to your location. Options include: <ul style="list-style-type: none"> <li>• US (Default)</li> <li>• EU</li> <li>• UK</li> </ul>                                                                                         |
| 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: <ul style="list-style-type: none"> <li>◦ Informational (default)</li> <li>◦ Low (default)</li> <li>◦ Medium (default)</li> <li>◦ High (default)</li> </ul> |

## Threat Intelligence Intel Profiles - Additional Parameter

| PARAMETER                | DESCRIPTION                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Context Ingestion Filter | Select the data you want ingested into ThreatQ. Options include: <ul style="list-style-type: none"> <li>• Related IOCs</li> <li>• WHOIS Information about related IOCs</li> </ul> |

## Threat Intelligence Articles - Additional Parameters

| PARAMETER                | DESCRIPTION                                                                                                                                                                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Context Ingestion Filter | <p>Select the data you want ingested into ThreatQ. Options include:</p> <ul style="list-style-type: none"> <li>• Related Attack Patterns</li> <li>• Related CVEs</li> <li>• Related CWE</li> <li>• Related IOCs</li> <li>• WHOIS Information about related IOCs</li> </ul> |
| Ingest CVEs As           | <p>Select the ThreatQ object type to ingest the CVEs as into ThreatQ. Options include:</p> <ul style="list-style-type: none"> <li>◦ Indicators</li> <li>◦ Vulnerabilities (default)</li> </ul>                                                                             |

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 365 Defender Incidents (Feed)

The Microsoft 365 Defender Incidents feed automatically pulls incidents, alerts, and related context from Microsoft 365 Defender.

GET <https://<region>.security.microsoft.com/api/incidents>

### 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":
"24c222b0b60fe148eece49ac83910cc6a7ef491",
                "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":
"24c222b0b60fe148eece49ac83910cc6a7ef491"
    }
  ]
}

```

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                              |
| .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                                                                |

| FEED DATA PATH                                    | THREATQ ENTITY       | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE                             | EXAMPLES                | NOTES                                 |
|---------------------------------------------------|----------------------|--------------------------------------|--------------------------------------------|-------------------------|---------------------------------------|
| <code>.value[].status</code>                      | Event.Attribute      | Status                               | <code>.value[].alerts[].createdTime</code> | Open                    | N/A                                   |
| <code>.value[].determination</code>               | Event.Attribute      | Determination                        | <code>.value[].alerts[].createdTime</code> | Unwanted Software       | Mapped to a more human-readable value |
| <code>.value[].comments[].comment</code>          | Event.Attribute      | Comment                              | <code>.value[].alerts[].createdTime</code> | N/A                     | N/A                                   |
| <code>.value[].detectionSource</code>             | Event.Attribute      | Detection Source                     | <code>.value[].alerts[].createdTime</code> | Microsoft Defender ATP  | Mapped to a more human-readable value |
| <code>.value[].assignedTo</code>                  | Event.Attribute      | Assigned To                          | <code>.value[].alerts[].createdTime</code> | N/A                     | N/A                                   |
| <code>.value[].alerts[].title</code>              | Event Title          | N/A                                  | <code>.alerts[].CreationTime</code>        | N/A                     | N/A                                   |
| <code>.value[].alerts[].description</code>        | Description          | N/A                                  | N/A                                        | N/A                     | N/A                                   |
| <code>.value[].alerts[].mitreTechniques</code>    | Attack Pattern.Value | N/A                                  | <code>.alerts[].CreationTime</code>        | N/A                     | N/A                                   |
| <code>.value[].alerts[].threatFamilyName</code>   | Malware.Value        | N/A                                  | <code>.alerts[].CreationTime</code>        | N/A                     | N/A                                   |
| <code>.value[].alerts[].actorName</code>          | Adversary.Value      | N/A                                  | <code>.alerts[].CreationTime</code>        | N/A                     | N/A                                   |
| <code>.value[].alerts[].serviceSource</code>      | Event.Attribute      | Service Source                       | <code>.alerts[].CreationTime</code>        | Office ATP              | Mapped to a more human-readable value |
| <code>.value[].alerts[].category</code>           | Event.Attribute      | Tactic                               | <code>.alerts[].CreationTime</code>        | Initial Access          | Mapped to a more human-readable value |
| <code>.value[].alerts[].status</code>             | Event.Attribute      | Status                               | <code>.alerts[].CreationTime</code>        | New                     | Mapped to a more human-readable value |
| <code>.value[].alerts[].severity</code>           | Event.Attribute      | Severity                             | <code>.alerts[].CreationTime</code>        | Medium                  | Mapped to a more human-readable value |
| <code>.value[].alerts[].investigationState</code> | Event.Attribute      | Investigation State                  | <code>.alerts[].CreationTime</code>        | Successfully Remediated | Mapped to a more human-readable value |
| <code>.value[].alerts[].classification</code>     | Event.Attribute      | Classification                       | <code>.alerts[].CreationTime</code>        | Not set                 | Mapped to a more human-readable value |

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

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

## Microsoft 365 Defender Threat Intelligence Articles

The Microsoft 365 Defender Threat Intelligence Articles feed pulls articles and related context from Microsoft Threat Intelligence.

GET <https://graph.microsoft.com/v1.0/security/threatIntelligence/articles>

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

## Microsoft 365 Defender Threat Intelligence Intel Profiles

The Microsoft 365 Defender Threat Intelligence Intel Profiles feed provides up-to-date threat actor infrastructure visibility.

GET <https://graph.microsoft.com/v1.0/security/threatIntelligence/intelProfiles>

### 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,<br>.value[].description.content,<br>.value[].tradecraft.content | Adversary/Tool/Report.Description | N/A                                  | N/A                          | Summary .value[].summary.content<br>Description .value[].description.content<br>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.                                                                |
| .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 365 Defender Threat Intelligence Indicators (supplemental)

The Intelligence Indicators supplemental feed will ingest related Indicators of compromise if you have selected the Related IOCs option selected under the **Context Ingestion Filter** for the Microsoft 365 Defender Threat Intelligence Intel Profiles and Articles feeds.

GET [https://graph.microsoft.com/v1.0/security/threatIntelligence/articles/{{ARTICLE\\_ID}}/indicators](https://graph.microsoft.com/v1.0/security/threatIntelligence/articles/{{ARTICLE_ID}}/indicators)

GET [https://graph.microsoft.com/v1.0/security/threatIntelligence/intelProfiles/{{PROFILE\\_ID}}/indicators](https://graph.microsoft.com/v1.0/security/threatIntelligence/intelProfiles/{{PROFILE_ID}}/indicators)

### Sample Response:

```
{
  "value": [
    {
      "id":
"aGFzaF9zaGEyNTYkJDMyMzIyNmQ2ZjljOTVmZGEzZDc0NWE5YmNlMWVjZDZiNTM4YjQzNTFhYTfjNm
ZkYTA1NDkzODhlZWm1ODVkJmJkHJpc2tpcQ==",
      "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":
"aGFzaF9tZDUkJDYwOWE5MjVmZDI1M2U4MmM4MDI2MmJhZDMxNmM3ZjE5JCRwdWJsaWM=",
      "source": "public"
    },
    {
      "artifact": {
        "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
        "id": "2d1ce0231cf8ff967c36bbfc931f3807ddba765c",
        "kind": "hash_sha1",
        "value": "2d1ce0231cf8ff967c36bbfc931f3807ddba765c"
      }
    }
  ]
}
```

```

    },
    "id":
"aGFzaF9zaGExJCQyZDFjZTAyMzFjZjhmZjk2N2MzMmJiZmM5MzFmMzgwN2RkYmE3NjVjJCRwdWJsaW
M=",
    "source": "public"
  },
  {
    "artifact": {
      "@odata.type": "#microsoft.graph.security.unclassifiedArtifact",
      "id": "keishagrey994@outlook.com",
      "kind": "email",
      "value": "keishagrey994@outlook.com"
    },
    "id": "ZW1haWwkJGtlaXNoYWdyZXk50TRAb3V0bG9vay5jb20kJHB1YmxpYw==",
    "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": "aXBfcG9ydCQkMTg1LjE1Ni43Mi4440jk40TAKJHB1YmxpYw==",
    "source": "public"
  },
  {
    "artifact": {
      "@odata.type": "#microsoft.graph.security.ipAddress",
      "id": "85.187.128.19"
    },
    "id": "aXAkJDg1LjE4Ny4xMjguMTk0JHB1YmxpYw==",
    "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[]<br>.artifact.value  | Indicator.Value     | .value[].artifact.kind               | .value[].firstSeenDateTime | 323226d6f9c95fda3d7<br>45a9bce1ecd6b538b4351aa1c6fda0549388eec585d63 | If value[].artifact.@dataType is #microsoft.graph.security.unclassifiedArtifact the mapping is done according to Microsoft Unclassified Artifacts mapping |
| .value[]<br>.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[]<br>.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 365 Defender Threat Intelligence Host WHOIS (supplemental)

The Threat Intelligence Host WHOIS supplemental feed will ingest 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 365 Defender Threat Intelligence Intel Profiles and Articles feeds.

GET [https://graph.microsoft.com/v1.0/security/threatIntelligence/hosts/{{HOST\\_ID}}/whois](https://graph.microsoft.com/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\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                     |
|-------------------------------------|---------------------|--------------------------------------|-------------------|-----------------------------------|---------------------------|
| .registrationDate                   | Indicator.Attribute | Registration Date                    | .registrationDate | 2023-06-22T00:52:33Z              | N/A                       |
| .lastUpdateDate                     | Indicator.Attribute | WHOIS Last Update                    | .registrationDate | 2023-10-24T11:06:15.164Z          | Updated if already exists |
| .whoisServer                        | Indicator.Attribute | WHOIS Server                         | .registrationDate | whois.auda.org.au                 | N/A                       |
| .domainStatus                       | Indicator.Attribute | Domain Status                        | .registrationDate | serverRenewProhibited...          | Updated if already exists |
| .registrant.email                   | Indicator.Attribute | Registrant Email                     | .registrationDate | abuse@key-systems.net             | N/A                       |
| .registrant.name                    | Indicator.Attribute | Registrant Name                      | .registrationDate | Ejay Turner                       | N/A                       |
| .registrant.organization            | Indicator.Attribute | Registrant Organization              | .registrationDate | PERPETUAL TRUSTEE COMPANY LIMITED | N/A                       |
| .registrant.address.city            | Indicator.Attribute | Registrant City                      | .registrationDate | Sofia                             | Title cased               |
| .registrant.address.countryOrRegion | Indicator.Attribute | Registrant Country                   | .registrationDate | Bulgaria                          | Title cased               |
| .registrant.address.postalCode      | Indicator.Attribute | Registrant Postal Code               | .registrationDate | N/A                               | N/A                       |
| .registrant.address.state           | Indicator.Attribute | Registrant State                     | .registrationDate | N/A                               | N/A                       |
| .registrant.address.street          | Indicator.Attribute | Registrant Street                    | .registrationDate | 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 365 Defender 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 365 Defender Threat Intelligence Articles

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

## Microsoft 365 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 365 Defender Threat Intelligence Articles** and **Microsoft 365 Defender Threat Intelligence Intel Profiles** feeds.

# Change Log

- **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