ThreatQuotient

A Securonix Company



ThreatQ Action Bundle for Microsoft Defender Threat Intelligence

Version 1.0.0

November 16, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **4**
Support **5**
Integration Details **6**
Introduction **7**
Prerequisites **10**
Installation **11**
Configuration **12**
All Actions Parameters 12
Microsoft Defender Threat Intel WHOIS Lookup - Additional Parameter 13
Microsoft Defender Threat Intel Forward Passive DNS - Additional Parameter 13
Microsoft Defender Threat Intel Article Details - Additional Parameter 13
Microsoft Defender Threat Intel Article Indicators - Additional Parameter 14
Microsoft Defender Threat Intel Intel Profile Details - Additional Parameter 14
Microsoft Defender Threat Intel Intel Profile Indicators - Additional Parameter 14
Microsoft Defender Threat Intel Host Port Details - Additional Parameter 14
Microsoft Defender Threat Intel WHOIS Record Details - Additional Parameter 15
Actions **16**
Microsoft Defender Threat Intel Host Details 18
Microsoft Defender Threat Intel Host Reputation 19
Microsoft Defender Threat Intel WHOIS Lookup 21
Microsoft Defender Threat Intel WHOIS History 23
Microsoft Defender Threat Intel Forward Passive DNS 26
Microsoft Defender Threat Intel Reverse Passive DNS 28
Microsoft Defender Threat Intel Host Cookies 30
Microsoft Defender Threat Intel Host Components 32
Microsoft Defender Threat Intel Host Pairs 34
Microsoft Defender Threat Intel Parent Host Pairs 36
Microsoft Defender Threat Intel Child Host Pairs 38
Microsoft Defender Threat Intel Host Ports 40
Microsoft Defender Threat Intel Host SSL Certificates 42
Microsoft Defender Threat Intel Host Trackers 44
Microsoft Defender Threat Intel Subdomains 46
Microsoft Defender Threat Intel Articles 47
Microsoft Defender Threat Intel Article Details 49
Microsoft Defender Threat Intel Article Indicators 51
Microsoft Defender Threat Intel Intel Profiles 53
Microsoft Defender Threat Intel Intel Profile Details 55
Microsoft Defender Threat Intel Intel Profile Indicators 57
Microsoft Defender Threat Intel Vulnerability 59
Microsoft Defender Threat Intel Vulnerability Components 62
Microsoft Defender Threat Intel Host Port Details 63
Microsoft Defender Threat Intel SSL Certificates 66
Microsoft Defender Threat Intel WHOIS Records 68
Microsoft Defender Threat Intel WHOIS Record Details 70
Enriched Data **72**
Microsoft Defender Threat Intel Host Details 72
Microsoft Defender Threat Intel Host Reputation 72

Microsoft Defender Threat Intel WHOIS Lookup 72
Microsoft Defender Threat Intel WHOIS History 73
Microsoft Defender Threat Intel Forward Passive DNS 73
Microsoft Defender Threat Intel Reverse Passive DNS 73
Microsoft Defender Threat Intel Host Cookies 74
Microsoft Defender Threat Intel Host Components 74
Microsoft Defender Threat Intel Host Pairs 74
Microsoft Defender Threat Intel Parent Host Pairs 75
Microsoft Defender Threat Intel Child Host Pairs 75
Microsoft Defender Threat Intel Host Ports 75
Microsoft Defender Threat Intel Host SSL Certificates 76
Microsoft Defender Threat Intel Host Trackers 76
Microsoft Defender Threat Intel Subdomains 76
Microsoft Defender Threat Intel Articles 77
Microsoft Defender Threat Intel Article Details 77
Microsoft Defender Threat Intel Article Indicators 77
Microsoft Defender Threat Intel Intel Profiles 78
Microsoft Defender Threat Intel Intel Profile Details 78
Microsoft Defender Threat Intel Intel Profile Indicators 78
Microsoft Defender Threat Intel Vulnerability 79
Microsoft Defender Threat Intel Vulnerability Components 79
Microsoft Defender Threat Intel Host Port Details 79
Microsoft Defender Threat Intel SSL Certificates 80
Microsoft Defender Threat Intel WHOIS Records 80
Microsoft Defender Threat Intel WHOIS Record Details 80
Known Issues / Limitations 82
Change Log 83

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 © 2026 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@securonix.com
Support Web: https://ts.securonix.com
Support Phone: 703.574.9893

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

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

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

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Action Bundle for Microsoft Defender Threat Intelligence brings Microsoft threat intelligence into ThreatQ TDR workflows. Use its actions to investigate indicators and enrich ThreatQ records with host details, reputation, WHOIS data, passive DNS, certificates, ports, components, trackers, subdomains, related hosts, and vulnerability intelligence. You can also search Microsoft threat intelligence articles and profiles, retrieve their details, and find associated indicators.

The bundle maps available results to ThreatQ indicators, attributes, descriptions, and tags, giving analysts added context for investigation and enrichment. It supports FQDN, IP Address, and IPv6 Address indicators.

The integration provides the following actions:

- **Microsoft Defender Threat Intel Host Details** - Retrieves host properties and maps available values to ThreatQ indicator attributes.
- **Microsoft Defender Threat Intel Host Reputation** - Maps host classification, score, and applicable reputation rules to attributes.
- **Microsoft Defender Threat Intel WHOIS Lookup** - Retrieves WHOIS registration details for a host indicator.
- **Microsoft Defender Threat Intel WHOIS History** - Retrieves historical WHOIS records and maps available values to the original indicator.
- **Microsoft Defender Threat Intel Forward Passive DNS** - Retrieves forward Passive DNS records for a host and maps record details to the original indicator.
- **Microsoft Defender Threat Intel Reverse Passive DNS** - Retrieves reverse Passive DNS records for a host and maps record details to the original indicator.
- **Microsoft Defender Threat Intel Host Cookies** - Retrieves cookies observed on a host and maps their names, domains, and observation dates.
- **Microsoft Defender Threat Intel Host Components** - Retrieves host components and maps their names, versions, categories, and observation dates.
- **Microsoft Defender Threat Intel Host Pairs** - Retrieves host-pair relationships and maps relationship details to the original indicator.
- **Microsoft Defender Threat Intel Parent Host Pairs** - Retrieves host-pair relationships where the submitted host is the child.
- **Microsoft Defender Threat Intel Child Host Pairs** - Retrieves child host relationships where the submitted host is the parent.
- **Microsoft Defender Threat Intel Host Ports** - Retrieves observed ports, status, banners, and service details for a host.

- **Microsoft Defender Threat Intel Host SSL Certificates** - Retrieves SSL certificates associated with a host and maps certificate details to the indicator.
- **Microsoft Defender Threat Intel Host Trackers** - Retrieves Internet trackers observed on a host and maps tracker details to the indicator.
- **Microsoft Defender Threat Intel Subdomains** - Retrieves subdomains observed for a host and maps their IDs and first-seen dates to the indicator.
- **Microsoft Defender Threat Intel Articles** - Searches Microsoft Threat Intelligence articles for the submitted indicator and adds article details, tags, and formatted body content.
- **Microsoft Defender Threat Intel Article Details** - Retrieves an article by its Graph resource ID and adds article details, tags, and formatted body content.
- **Microsoft Defender Threat Intel Article Indicators** - Retrieves indicators related to the configured Microsoft Graph article and adds their source and artifact identifiers.
- **Microsoft Defender Threat Intel Intel Profiles** - Searches Microsoft Threat Intelligence intel profiles for the submitted indicator and maps profile details to its attributes.
- **Microsoft Defender Threat Intel Intel Profile Details** - Retrieves a Microsoft Graph intel profile by its resource ID and maps its profile details to the original indicator.
- **Microsoft Defender Threat Intel Intel Profile Indicators** - Retrieves indicators related to the configured Microsoft Graph intel profile and maps their source, dates, and artifact identifiers.
- **Microsoft Defender Threat Intel Vulnerability** - Retrieves vulnerability intelligence for a CVE and maps the returned details to the original indicator.
- **Microsoft Defender Threat Intel Vulnerability Components** - Retrieves components associated with a CVE and maps each component's ID and name to the original indicator.
- **Microsoft Defender Threat Intel Host Port Details** - Retrieves one host port by Graph resource ID, including banners, services, and associated host details.
- **Microsoft Defender Threat Intel SSL Certificates** - Searches SSL certificates by the submitted indicator as subject common name and maps certificate details to the indicator.
- **Microsoft Defender Threat Intel WHOIS Records** - Searches WHOIS records by nameserver host and maps registration details to the matching FQDN indicator.
- **Microsoft Defender Threat Intel WHOIS Record Details** - Retrieves one WHOIS record by Graph resource ID and maps its details to the original indicator.

The integration is compatible with the following indictor types:

- FQDN

- IP Address
- IPv6 Address

The integration enriches the following object types:

- Indicators
- Indicator Attributes
- Descriptions
- Tags



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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator types:
  - FQDN
  - IP Address
  - IPv6 Address
- A Microsoft Entra application registration with its tenant ID, client ID, and client secret.
- Microsoft Graph application permission `ThreatIntelligence.Read.All` and with tenant administrator consent.
- Ensure the tenant is entitled to access the Microsoft Defender Threat Intelligence API. If the API returns `402 Payment Required`, contact the tenant administrator to confirm access.



For permission details, see the Microsoft Threat Intelligence API overview.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

Configuration

ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

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

All Actions Parameters

The following configuration parameters are available for all actions:

PARAMETER	DESCRIPTION
Tenant ID	Your Microsoft Entra tenant ID.
Client ID	Your application (client) ID for the Entra app registration.
Client Secret	Your client secret for the app registration.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.

Microsoft Defender Threat Intel WHOIS Lookup - Additional Parameter

PARAMETER	DESCRIPTION
Include Raw WHOIS Text	When enabled, publishes raw WHOIS text, which may contain contact information.

Microsoft Defender Threat Intel Forward Passive DNS - Additional Parameter

PARAMETER	DESCRIPTION
Passive DNS Record Type	Filters records by type. Options include: ◦ `A` *(default)* ◦ `AAAA` ◦ `CNAME` ◦ `MX` ◦ `NS` ◦ `PTR` ◦ `SOA` ◦ `TXT`

Microsoft Defender Threat Intel Article Details - Additional Parameter

PARAMETER	DESCRIPTION
Related Graph Resource ID	Microsoft Graph article ID used to retrieve the article.

Microsoft Defender Threat Intel Article Indicators - Additional Parameter

PARAMETER	DESCRIPTION
Related Graph Resource ID	Microsoft Graph article ID whose related indicators are retrieved. Use the article's top-level `id`.

Microsoft Defender Threat Intel Intel Profile Details - Additional Parameter

PARAMETER	DESCRIPTION
Related Graph Resource ID	Microsoft Graph intel profile ID to retrieve. Use the profile's top-level `id` returned by Intel Profiles.

Microsoft Defender Threat Intel Intel Profile Indicators - Additional Parameter

PARAMETER	DESCRIPTION
Related Graph Resource ID	Microsoft Graph intel profile ID whose related indicators are retrieved. Use the profile's top-level `id`.

Microsoft Defender Threat Intel Host Port Details - Additional Parameter

PARAMETER	DESCRIPTION
Related Graph Resource ID	Microsoft Graph hostPort ID to retrieve. Use the `id` of a hostPort returned by Host Ports.

Microsoft Defender Threat Intel WHOIS Record Details - Additional Parameter

PARAMETER	DESCRIPTION
Related Graph Resource ID	Microsoft Graph WHOIS record ID to retrieve. Use the record's top-level `id` returned by WHOIS Records.

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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Microsoft Defender Threat Intel Host Details	Retrieves host properties and maps available values to ThreatQ indicator attributes.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel Host Reputation	Maps host classification, score, and applicable reputation rules to attributes.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel WHOIS Lookup	Retrieves WHOIS registration details for a host indicator.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel WHOIS History	Retrieves historical WHOIS records and maps available values to the original indicator.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel Forward Passive DNS	Retrieves forward Passive DNS records for a host and maps record details to the original indicator.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel Reverse Passive DNS	Retrieves reverse Passive DNS records for a host and maps record details to the original indicator.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel Host Cookies	Retrieves cookies observed on a host and maps their names, domains, and observation dates.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel Host Components	Retrieves host components and maps their names, versions, categories, and observation dates.	Indicator	FQDN, IP Address, IPv6 Address
Microsoft Defender Threat Intel Host Pairs	Retrieves host-pair relationships and maps relationship details to the	Indicator	FQDN, IP Address, IPv6 Address

Microsoft Defender Threat Intel Host Details

The Microsoft Defender Threat Intel Host Details action retrieves host metadata from Microsoft Graph and enriches the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/example.test",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#security/threatIntelligence/hosts/$entity",
  "@odata.type": "#microsoft.graph.security.hostname",
  "firstSeenDateTime": "2025-01-15T00:00:00Z",
  "id": "example.test",
  "lastSeenDateTime": "2026-08-20T12:00:00Z",
  "registrant": "Example Organization",
  "registrar": "Example Registrar"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2010-06-24T03:12:57Z	Earliest observation time returned by Graph.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-10-26T23:56:55.542Z	Most recent observation time returned by Graph.
.registrar	Indicator.Attribute	Registrar	N/A	Registrar name	Hostname registration property.
.registrant	Indicator.Attribute	Registrant	N/A	Registrant name	Hostname registration property.

Microsoft Defender Threat Intel Host Reputation

The Microsoft Defender Threat Intel Host Reputation action retrieves the reputation of a host and maps its classification and score to separate attributes on the original indicator. The rules attribute is added when Microsoft returns one or more rules.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/fake-malicious.site/reputation",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#security/threatIntelligence/hosts('fake-
malicious.site')/reputation/$entity",
  "@odata.type": "#microsoft.graph.security.hostReputation",
  "id": "1e3b9ded-abb6-1828-c4ef-a5ca48b287a0",
  "classification": "malicious",
  "score": 100,
  "rules": [
    {
      "name": "Microsoft Defender Threat Intelligence Intel Article",
      "description": "Activity Snapshot: DPRK Actors Target Maritime
Sector",
      "severity": "high",
      "relatedDetailsUrl": "https://ti.defender.microsoft.com/
article/831b70a4"
    },
    {
      "name": "Name server",
      "description": "Domain is using a name server that has been
associated with suspicious behavior",
      "severity": "medium",
      "relatedDetailsUrl": null
    },
```

```
    {
      "name": "Resolving IP Address",
      "description": "192.168.1.1",
      "severity": "low",
      "relatedDetailsUrl": "https://ti.defender.microsoft.com/search?
query=192.168.1.1"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.classification	Indicator.Attribute	Classification	N/A	malicious	Calculated classification: unknown, neutral, suspicious, or malicious.
.score	Indicator.Attribute	Score	N/A	100	Range 0 to 100. Zero is retained as a valid score.
.rules[].name	Indicator.Attribute	Rule Name	N/A	One rule name per value	Attribute name repeats once per rule.
.rules[].description	Indicator.Attribute	Rule Description	N/A	One description per value	Attribute name repeats once per rule.
.rules[].severity	Indicator.Attribute	Rule Severity	N/A	One severity per value	Attribute name repeats once per rule.
.rules[].relatedDetailsUrl	Indicator.Attribute	Rule Related Details URL	N/A	One URL per value	Attribute name repeats for rules that have a URL.

Microsoft Defender Threat Intel WHOIS Lookup

The Microsoft Defender Threat Intel WHOIS Lookup action retrieves the current WHOIS record for a host and attaches available registration details to the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/example.test/whois",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.type": "#microsoft.graph.security.whoisRecord",
  "id": "sample-whois-record-id",
  "domainStatus": "client transfer prohibited",
  "expirationDateTime": "2027-01-02T00:00:00Z",
  "firstSeenDateTime": "2020-01-02T00:00:00Z",
  "lastSeenDateTime": "2026-08-14T10:30:00Z",
  "lastUpdateDateTime": "2026-08-14T10:30:00Z",
  "registrationDateTime": "2020-01-02T00:00:00Z",
  "whoisServer": "whois.example.test",
  "registrar": {
    "@odata.type": "microsoft.graph.security.whoisContact",
    "name": "Example Registrar"
  },
  "registrant": {
    "@odata.type": "microsoft.graph.security.whoisContact",
    "name": "Example Registrant",
    "organization": "Example Organization"
  },
  "admin": {
    "@odata.type": "microsoft.graph.security.whoisContact",
    "name": "Example Administrator"
  },
  "technical": {
    "@odata.type": "microsoft.graph.security.whoisContact",
```

```
    "name": "Example Technical Contact"
  },
  "abuse": {
    "@odata.type": "microsoft.graph.security.whoisContact",
    "name": "Abuse Contact"
  },
  "nameservers": [
    {
      "@odata.type": "microsoft.graph.security.whoisNameserver",
      "firstSeenDateTime": "2020-01-02T00:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:30:00Z",
      "host": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "ns1.example.test"
      }
    }
  ],
  "rawWhoisText": "Example WHOIS text with contact values redacted."
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.domainStatus	Indicator.Attribute	Domain Status	N/A	client update prohibited,client transfer prohibited,client delete prohibited	Registration status values returned by Microsoft Graph.
.registrationDateTime	Indicator.Attribute	Registration Date Time	N/A	1998-09-01T04:00:00Z	Registration date and time.
.expirationDateTime	Indicator.Attribute	Expiration Date Time	N/A	2027-08-31T00:00:00Z	Expiration date and time.
.lastUpdateDateTime	Indicator.Attribute	Last Update Date Time	N/A	2026-09-30T23:00:18.858Z	Most recent record update time.
.whoisServer	Indicator.Attribute	WHOIS Server	N/A	whois.markmonitor.com	WHOIS server associated with the record.
.registrar.name	Indicator.Attribute	Registrar Name	N/A	Markmonitor Inc.	Registrar name, when returned.
.registrant.name	Indicator.Attribute	Registrant Name	N/A	Domain Administrator	Registrant name, when returned.
.rawWhoisText	Indicator.Attribute	Raw WHOIS Text	N/A	WHOIS registration text	Published only when **Include Raw WHOIS Text** is enabled.

Microsoft Defender Threat Intel WHOIS History

The Microsoft Defender Threat Intel WHOIS History action retrieves historical WHOIS records for a host and adds available values to the original indicator. Each returned history record is processed individually, so attribute names repeat when multiple records provide the same field.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/example.test/whois/history",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#Collection(microsoft.graph.security.whoisHistoryRecord
)",
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.whoisHistoryRecord",
      "id": "sample-whois-history-record-id",
      "domainStatus": "server delete prohibited,server update
prohibited,server transfer prohibited",
      "registrationDateTime": "1995-06-05T00:00:00Z",
      "expirationDateTime": "2027-12-08T17:00:53Z",
      "firstSeenDateTime": null,
      "lastSeenDateTime": null,
      "lastUpdateDateTime": "2026-09-30T06:52:35.335Z",
      "whoisServer": "whois.example.test",
      "registrar": {
        "@odata.type": "#microsoft.graph.security.whoisContact",
        "name": "Example Registrar",
        "organization": "Example Registrar"
      },
      "registrant": {
        "@odata.type": "#microsoft.graph.security.whoisContact",
```

```
        "name": "Example Registrant",
        "organization": "Example Organization"
      },
      "nameservers": [
        {
          "@odata.type": "#microsoft.graph.security.whoisNameserver",
          "firstSeenDateTime": null,
          "lastSeenDateTime": null,
          "host": {
            "@odata.type": "#microsoft.graph.security.hostname",
            "id": "ns1.example.test"
          }
        },
        {
          "@odata.type": "#microsoft.graph.security.whoisNameserver",
          "firstSeenDateTime": null,
          "lastSeenDateTime": null,
          "host": {
            "@odata.type": "#microsoft.graph.security.hostname",
            "id": "ns2.example.test"
          }
        }
      ],
      "rawWhoisText": "WHOIS text redacted for privacy."
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.domainStatus	Indicator.Attribute	Domain Status	N/A	server delete prohibited,...	One value per record; attribute name repeats across records.
.registrationDateTime	Indicator.Attribute	Registration Date Time	N/A	1995-06-05T00:00:00Z	Published when the record provides a value.
.expirationDateTime	Indicator.Attribute	Expiration Date Time	N/A	2027-12-08T17:00:53Z	Published when the record provides a value.
.lastUpdateDateTime	Indicator.Attribute	Last Update Date Time	N/A	2026-09-30T06:52:35.335Z	Published when the record provides a value.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	null	Omitted when Microsoft Graph returns null.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	null	Omitted when Microsoft Graph returns null.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.whoisServer	Indicator.Attribute	WHOIS Server	N/A	whois.example.test	Published when the record provides a value.
.registrar.name	Indicator.Attribute	Registrar Name	N/A	Example Registrar	Published when the registrar name is available.
.registrant.name	Indicator.Attribute	Registrant Name	N/A	Example Registrant	Published when the registrant name is available.
.registrant.organization	Indicator.Attribute	Registrant Organization	N/A	Example Organization	Published when the registrant organization is available.
.nameservers[].host.id	Indicator.Attribute	Nameserver Host ID	N/A	ns1.example.test; ns2.example.test	N/A

Microsoft Defender Threat Intel Forward Passive DNS

The Microsoft Defender Threat Intel Forward Passive DNS action retrieves forward Passive DNS records for a host. Select a DNS record type to filter the results; the default is `A`.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/kernel.org/passiveDns",
  "params": {
    "$filter": "recordType eq 'A'"
  },
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#Collection(microsoft.graph.security.passiveDnsRecord)"
,
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.passiveDnsRecord",
      "id": "sample-passive-dns-id",
      "collectedDateTime": "2026-08-14T10:30:00Z",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "recordType": "A",
      "artifact": {
        "@odata.type": "#microsoft.graph.security.ipAddress",
        "id": "192.0.2.10"
      },
      "parentHost": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "kernel.org"
      }
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.recordType	Indicator.Attribute	Record Type	N/A	A	Record type is selected in the feed configuration.
.collectedDateTime	Indicator.Attribute	Collected Date Time	N/A	2026-08-14T10:30:00Z	Collection time returned for the record.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.artifact.id	Indicator.Attribute	Artifact ID	N/A	192.0.2.10	Resolved artifact associated with the DNS record.
.parentHost.id	Indicator.Attribute	Parent Host ID	N/A	example.test	Host associated with the Passive DNS record.

Microsoft Defender Threat Intel Reverse Passive DNS

The Microsoft Defender Threat Intel Reverse Passive DNS action retrieves reverse Passive DNS records for a host indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/192.0.2.10/passiveDnsReverse",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#Collection(microsoft.graph.security.passiveDnsRecord)"
,
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.passiveDnsRecord",
      "id": "sample-reverse-passive-dns-id",
      "collectedDateTime": "2026-08-14T10:30:00Z",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "recordType": "A",
      "artifact": {
        "@odata.type": "#microsoft.graph.security.ipAddress",
        "id": "192.0.2.10"
      },
      "parentHost": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "example.test"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.recordType	Indicator.Attribute	Record Type	N/A	A	DNS record type returned by Graph.
.collectedDateTime	Indicator.Attribute	Collected Date Time	N/A	2026-08-14T10:30:00Z	Collection time returned for the record.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.artifact.id	Indicator.Attribute	Artifact ID	N/A	192.0.2.10	Artifact associated with the DNS record.
.parentHost.id	Indicator.Attribute	Parent Host ID	N/A	example.test	Host associated with the Passive DNS record.

Microsoft Defender Threat Intel Host Cookies

The Microsoft Defender Threat Intel Host Cookies action retrieves cookies observed on a host and attaches available cookie details to the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/wikipedia.org/cookies",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#Collection(microsoft.graph.security.hostCookie)",
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostCookie",
      "id": "sample-cookie-id",
      "domain": "wikipedia.org",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "name": "SESSIONID",
      "host": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "wikipedia.org"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Indicator.Attribute	Name	N/A	SESSIONID	Cookie name returned by Microsoft Graph.
.domain	Indicator.Attribute	Domain	N/A	wikipedia.org	Cookie domain.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.

Microsoft Defender Threat Intel Host Components

The Microsoft Defender Threat Intel Host Components action retrieves web components associated with a host and attaches available details to the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/example.test/components",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostComponent",
      "id": "sample-component-id",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "name": "Example Server",
      "version": "1.0",
      "category": "Server",
      "host": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "example.test"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Indicator.Attribute	Name	N/A	Example Server	Component name reported for the host.
.version	Indicator.Attribute	Version	N/A	1.0	Component version.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.category	Indicator.Attribute	Category	N/A	Server	Component category.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.

Microsoft Defender Threat Intel Host Pairs

The Microsoft Defender Threat Intel Host Pairs action retrieves parent-child host relationships associated with a host and attaches available details to the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/example.test/hostPairs",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostPair",
      "id": "sample-host-pair-id",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "linkKind": "redirect",
      "parentHost": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "example.test"
      },
      "childHost": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "destination.example.test"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.linkKind	Indicator.Attribute	Link Kind	N/A	redirect	Reason for the host-pair relationship.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.parentHost.id	Indicator.Attribute	Parent Host ID	N/A	example.test	Host that led to the child host.
.childHost.id	Indicator.Attribute	Child Host ID	N/A	destination.example.test	Host reached through the parent host.

Microsoft Defender Threat Intel Parent Host Pairs

The Microsoft Defender Threat Intel Parent Host Pairs action retrieves host-pair records where the submitted host is the child and maps each returned relationship to the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/destination.example.test/parentHostPairs",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostPair",
      "id": "sample-host-pair-id",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "linkKind": "redirect",
      "parentHost": {
        "id": "example.test"
      },
      "childHost": {
        "id": "destination.example.test"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.linkKind	Indicator.Attribute	Link Kind	N/A	redirect	Relationship type, when returned.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time for the relationship.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.parentHost.id	Indicator.Attribute	Parent Host ID	N/A	example.test	Host that led to the submitted child host.
.childHost.id	Indicator.Attribute	Child Host ID	N/A	destination.example.test	Submitted host reached through the parent host.

Microsoft Defender Threat Intel Child Host Pairs

The Microsoft Defender Threat Intel Child Host Pairs action retrieves host-pair records where the submitted host is the parent and maps each returned relationship to the original indicator. Testing with `akamai.com` created 101 indicator attributes. Parent and child host IDs and observation dates repeat across the returned relationships.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/akamai.com/childHostPairs",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostPair",
      "id": "sample-host-pair-id",
      "firstSeenDateTime": "2022-05-11T01:27:14.187Z",
      "lastSeenDateTime": "2023-06-23T06:33:31.493Z",
      "linkKind": "finalRedirect",
      "parentHost": {
        "id": "akamai.com"
      },
      "childHost": {
        "id": "destination.akamai.com"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.linkKind`	`Indicator.Attribute`	`Link Kind`	`N/A`	`finalRedirect`	`Relationship type, when returned.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2025-07-30T00:59:28.206Z	First observation time for the relationship.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-10-26T23:58:47.172Z	Most recent observation time.
.parentHost.id	Indicator.Attribute	Parent Host ID	N/A	*.pattd.akamai.com	Host that led to the child host.
.childHost.id	Indicator.Attribute	Child Host ID	N/A	*.pattd.akamai.com	Host reached through the parent host.

Microsoft Defender Threat Intel Host Ports

The Microsoft Defender Threat Intel Host Ports action retrieves observed port information for a host and attaches available details to the original indicator. A successful test with `microsoft.com` returned no port records, so no attributes were added in that run.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/microsoft.com/ports",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostPort",
      "id": "ODUuMTMuMTM5LjE4JCQ0NDM=",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "lastScanDateTime": "2026-08-14T10:30:00Z",
      "port": 443,
      "protocol": "tcp",
      "status": "open",
      "timesObserved": 42,
      "banners": [
        {
          "banner": "HTTP/1.1 200 OK",
          "firstSeenDateTime": "2026-08-01T10:00:00Z",
          "lastSeenDateTime": "2026-08-14T10:25:00Z",
          "scanProtocol": "https",
          "timesObserved": 4
        }
      ],
      "services": [
        {
```

```
          "firstSeenDateTime": "2026-08-01T10:00:00Z",
          "lastSeenDateTime": "2026-08-14T10:25:00Z",
          "isRecent": true,
          "component": {
            "id": "sample-component-id",
            "name": "Example Server",
            "version": "1.0",
            "category": "Server"
          }
        }
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.port	Indicator.Attribute	Port	N/A	443	Observed host port.
.protocol	Indicator.Attribute	Protocol	N/A	tcp	Protocol reported for the port.
.status	Indicator.Attribute	Status	N/A	open	Port status reported by Microsoft Graph.
.timesObserved	Indicator.Attribute	Times Observed	N/A	42	Number of observations.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.lastScanDateTime	Indicator.Attribute	Last Scan Date Time	N/A	2026-08-14T10:30:00Z	Most recent scan time.
.banners	Indicator.Attribute	Banners	N/A	Banner records	Banner data returned for the port.
.services	Indicator.Attribute	Services	N/A	Service records	Service component data returned for the port.

Microsoft Defender Threat Intel Host SSL Certificates

The Microsoft Defender Threat Intel Host SSL Certificates action retrieves SSL certificates associated with a host and attaches available certificate details to the original indicator. Testing with `cloudflare.com` completed successfully and created 160 indicator attributes. Certificate IDs, fingerprints, SHA1 values, and date attributes repeat across returned certificates.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/cloudflare.com/sslCertificates",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostSslCertificate",
      "id": "sample-host-ssl-certificate-id",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "ports": [
        {
          "port": 443,
          "firstSeenDateTime": "2026-01-10T08:00:00Z",
          "lastSeenDateTime": "2026-08-14T10:25:00Z"
        }
      ],
      "sslCertificate": {
        "id": "sample-ssl-certificate-id",
        "expirationDateTime": "2027-08-01T00:00:00Z",
        "fingerprint":
"fb:96:55:15:05:f1:ed:b2:4d:d3:b3:6f:cf:fd:b7:65:83:3b:81:18",
        "sha1": "fb96551505f1edb24dd3b36fcffdb765833b8118",
        "subject": {
          "commonName": "cloudflare.com"
```

```
        },
        "issuer": {
          "commonName": "Example Certificate Authority"
        }
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time for the host-certificate link.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time for the link.
.ports	Indicator.Attribute	Ports	N/A	443	Port values associated with the certificate link.
.sslCertificate.id	Indicator.Attribute	SSL Certificate ID	N/A	sample-ssl-certificate-id	Certificate identifier.
.sslCertificate.fingerprint	Indicator.Attribute	SSL Certificate Fingerprint	N/A	fb:96:55:15:05:f1:ed:b2:4d:d3:b3:6f:cf:fd:b7:65:83:3b:81:18	Certificate fingerprint.
.sslCertificate.sha1	Indicator.Attribute	SSL Certificate SHA1	N/A	fb96551505f1edb24dd3b36fcffdb765833b8118	SHA1 hash of the certificate.
.sslCertificate.expirationDateTime	Indicator.Attribute	SSL Certificate Expiration Date Time	N/A	2027-08-01T00:00:00Z	Certificate expiration time.
.sslCertificate.subject.commonName	Indicator.Attribute	SSL Certificate Subject Common Name	N/A	cloudflare.com	Certificate subject common name.
.sslCertificate.issuer.commonName	Indicator.Attribute	SSL Certificate Issuer Common Name	N/A	Example Certificate Authority	Certificate issuer common name.

Microsoft Defender Threat Intel Host Trackers

The Microsoft Defender Threat Intel Host Trackers action retrieves Internet trackers observed on a host and attaches tracker details to the original indicator. Testing with `akamai.net` completed successfully and created 60 indicator attributes. Tracker values and their first-seen and last-seen dates repeat across returned records.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/akamai.net/trackers",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.hostTracker",
      "id": "sample-tracker-id",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "kind": "GoogleAnalyticsID",
      "value": "G-EXAMPLE1234",
      "host": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "akamai.net"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.kind`	`Indicator.Attribute`	`Kind`	`N/A`	`BitlyId`	`Tracker type reported by Graph.`
`.value`	`Indicator.Attribute`	`Value`	`N/A`	`githubstatus`	`Tracker identifier or value.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2016-12-27T02:30:39.774Z	First observation time for the tracker.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2020-07-31T21:28:45.293Z	Most recent observation time.

Microsoft Defender Threat Intel Subdomains

The Microsoft Defender Threat Intel Subdomains action retrieves subdomain records associated with a host and attaches each record's ID and first-seen date to the original indicator. Testing with `github.com` completed successfully and created 36 indicator attributes, with IDs and first-seen dates repeating across returned records.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hosts/github.com/subdomains",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.subdomain",
      "id": "Z2l0aHVlLmNvbSQkZ2l0aHVlLmNvbQ==",
      "firstSeenDateTime": "2010-06-24T04:40:37Z",
      "host": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "github.com"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.id`	`Indicator.Attribute`	`ID`	`N/A`	`Z2l0aHVlLmNvbSQkZ2l0aHVlLmNvbQ==`	`Identifier for the returned subdomain.`
`.firstSeenDateTime`	`Indicator.Attribute`	`First Seen Date Time`	`N/A`	`2010-06-24T04:40:37Z`	`First observation time for the subdomain.`

Microsoft Defender Threat Intel Articles

The Microsoft Defender Threat Intel Articles action searches Microsoft Graph threat intelligence articles using the submitted FQDN or IP indicator. Article metadata is mapped to indicator attributes, Microsoft article tags are added as indicator tags, and the formatted article body is added to the indicator description.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/articles?$search=\"example.test\"",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.article",
      "id": "sample-article-id",
      "createdDateTime": "2025-01-15T12:00:00Z",
      "lastUpdatedDateTime": "2025-02-01T09:30:00Z",
      "isFeatured": false,
      "imageUrl": "https://example.test/images/article.png",
      "title": "Example threat intelligence article",
      "summary": {
        "content": "A concise summary of the reported activity.",
        "format": "markdown"
      },
      "body": {
        "content": "Example article body for a threat report.",
        "format": "markdown"
      },
      "tags": ["phishing", "infrastructure"]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Indicator.Attribute	Title	N/A	Example threat intelligence article	Published when the article has a title.
.createdDateTime	Indicator.Attribute	Created Date Time	N/A	2025-01-15T12:00:00Z	Article creation time.
.lastUpdatedDateTime	Indicator.Attribute	Last Updated Date Time	N/A	2025-02-01T09:30:00Z	Most recent article update time.
.isFeatured	Indicator.Attribute	Is Featured	N/A	true	Published when the value is true.
.imageUrl	Indicator.Attribute	Image URL	N/A	https://example.test/images/article.png	Article image URL.
.summary.content	Indicator.Attribute	Summary Content	N/A	A concise summary of the reported activity.	Summary text from the formatted content object.
.body.content	Indicator.Description	Description	N/A	Example article body for a threat report.	Cleaned with the shared description formatter.
.tags[]	Indicator.Tag	Tag	N/A	phishing, infrastructure	Each returned tag is added to the indicator as a tag.

Microsoft Defender Threat Intel Article Details

The Microsoft Defender Threat Intel Article Details action retrieves one Microsoft Graph threat intelligence article using the configured Graph resource ID. Article metadata and tags are added to the original indicator, and the formatted article body is added to its description.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/articles/sample-article-id",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.type": "#microsoft.graph.security.article",
  "id": "sample-article-id",
  "createdDateTime": "2025-01-15T12:00:00Z",
  "lastUpdatedDateTime": "2025-02-01T09:30:00Z",
  "isFeatured": false,
  "imageUrl": "https://example.test/images/article.png",
  "title": "Example threat intelligence article",
  "summary": {
    "content": "A concise summary of the reported activity.",
    "format": "markdown"
  },
  "body": {
    "content": "Example article body for a threat report.",
    "format": "markdown"
  },
  "tags": ["phishing", "infrastructure"]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	`Indicator.Attribute`	`Title`	`N/A`	`Example threat intelligence article`	`Published when the article has a title.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.createdDateTime	Indicator.Attribute	Created Date Time	N/A	2025-01-15T12:00:00Z	Article creation time.
.lastUpdatedDateTime	Indicator.Attribute	Last Updated Date Time	N/A	2025-02-01T09:30:00Z	Most recent article update time.
.isFeatured	Indicator.Attribute	Is Featured	N/A	true	Published when the value is true.
.imageUrl	Indicator.Attribute	Image URL	N/A	https://example.test/images/article.png	Article image URL.
.summary.content	Indicator.Attribute	Summary Content	N/A	A concise summary of the reported activity.	Summary text from the formatted content object.
.body.content	Indicator.Description	Description	N/A	Example article body for a threat report.	Cleaned with the shared description formatter.
.tags[]	Indicator.Tag	Tag	N/A	phishing, infrastructure	Each returned tag is added to the indicator as a tag.

Microsoft Defender Threat Intel Article Indicators

The Microsoft Defender Threat Intel Article Indicators action retrieves indicators associated with the article identified by **Related Graph Resource ID** and adds the returned indicator source and artifact identifiers as attributes on the original FQDN or IP indicator. Enter the article's top-level `id` returned by Microsoft Defender Threat Intel Articles; the submitted ThreatQ indicator value is separate from this field.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/articles/sample-article-id/indicators",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.articleIndicator",
      "id": "ZmFrZS1tYWxpY2lvdXMuc2l0ZQ==",
      "source": "microsoft",
      "artifact": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "fake-malicious.site"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.source`	`Indicator.Attribute`	`Source`	`N/A`	`microsoft`	`Source of the related article indicator.`
`.artifact.id`	`Indicator.Attribute`	`Artifact ID`	`N/A`	`fake-malicious.site`	`Value of the related artifact.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.id	Indicator.Attribute	ID	N/A	ZmFrZS1tYWxpY2lvdXMuc2l0ZQ==	Microsoft Graph ID of the article indicator.

Microsoft Defender Threat Intel Intel Profiles

The Microsoft Defender Threat Intel Intel Profiles action searches Microsoft Graph intelligence profiles using the submitted FQDN or IP indicator and maps returned profile details to attributes on the original indicator. This action uses the Microsoft Graph `$search` parameter.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/intelProfiles?$search=\"protonmail.ch\"",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.intelligenceProfile",
      "id": "sample-intel-profile-id",
      "aliases": ["Example Actor"],
      "description": {
        "@odata.type": "microsoft.graph.security.formattedContent",
        "content": "Example actor profile description.",
        "format": "markdown"
      },
      "firstActiveDateTime": "2020-01-01T00:00:00Z",
      "kind": "actor",
      "summary": {
        "@odata.type": "microsoft.graph.security.formattedContent",
        "content": "Example actor profile summary.",
        "format": "markdown"
      },
      "targets": ["Technology"],
      "title": "Example Threat Actor",
      "tradecraft": {
        "@odata.type": "microsoft.graph.security.formattedContent",
        "content": "Example tactics, techniques, and procedures.",
```

```
        "format": "markdown"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Indicator.Attribute	Title	N/A	Example Threat Actor	Title of the intelligence profile.
.kind	Indicator.Attribute	Kind	N/A	actor	Profile kind.
.id	Indicator.Attribute	ID	N/A	sample-intel-profile-id	Microsoft Graph profile identifier.
.firstActiveDateTime	Indicator.Attribute	First Active Date Time	N/A	2020-01-01T00:00:00Z	First known activity date.
.aliases[]	Indicator.Attribute	Aliases	N/A	Example Actor	One attribute value per alias; name repeats for multiple aliases.
.targets[]	Indicator.Attribute	Targets	N/A	Technology	One attribute value per target; name repeats for multiple targets.
.description.content	Indicator.Attribute	Description Content	N/A	Example actor profile description.	Content from the formatted profile description.
.summary.content	Indicator.Attribute	Summary Content	N/A	Example actor profile summary.	Content from the formatted profile summary.
.tradecraft.content	Indicator.Attribute	Tradecraft Content	N/A	Example tactics, techniques, and procedures.	Content from the formatted tradecraft details.
.countriesOrRegionsOfOrigin[]	Indicator.Attribute	Countries Or Regions Of Origin	N/A	Country or region value	One attribute value per country or region.

Microsoft Defender Threat Intel Intel Profile Details

The Microsoft Defender Threat Intel Intel Profile Details action retrieves the intelligence profile identified by **Related Graph Resource ID** and maps its available details to attributes on the original FQDN or IP indicator. Use the profile's top-level `id` returned by Microsoft Defender Threat Intel Intel Profiles; the submitted indicator value is separate from this field.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/intelProfiles/sample-intel-profile-id",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.type": "#microsoft.graph.security.intelligenceProfile",
  "id": "sample-intel-profile-id",
  "aliases": ["Example Actor"],
  "description": {
    "@odata.type": "microsoft.graph.security.formattedContent",
    "content": "Example actor profile description.",
    "format": "markdown"
  },
  "firstActiveDateTime": "2020-01-01T00:00:00Z",
  "kind": "actor",
  "summary": {
    "@odata.type": "microsoft.graph.security.formattedContent",
    "content": "Example actor profile summary.",
    "format": "markdown"
  },
  "targets": ["Technology"],
  "title": "Example Threat Actor",
  "tradecraft": {
    "@odata.type": "microsoft.graph.security.formattedContent",
    "content": "Example tactics, techniques, and procedures.",
    "format": "markdown"
```

```
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Indicator.Attribute	Title	N/A	Example Threat Actor	Title of the intelligence profile.
.kind	Indicator.Attribute	Kind	N/A	actor	Profile kind.
.id	Indicator.Attribute	ID	N/A	sample-intel-profile-id	Microsoft Graph profile identifier.
.firstActiveDateTime	Indicator.Attribute	First Active Date Time	N/A	2020-01-01T00:00:00Z	First known activity date.
.aliases[]	Indicator.Attribute	Aliases	N/A	Example Actor	One attribute value per alias; name repeats for multiple aliases.
.targets[]	Indicator.Attribute	Targets	N/A	Technology	One attribute value per target; name repeats for multiple targets.
.description.content	Indicator.Attribute	Description Content	N/A	Example actor profile description.	Content from the formatted profile description.
.summary.content	Indicator.Attribute	Summary Content	N/A	Example actor profile summary.	Content from the formatted profile summary.
.tradecraft.content	Indicator.Attribute	Tradecraft Content	N/A	Example tactics, techniques, and procedures.	Content from the formatted tradecraft details.
.countriesOrRegionsOfOrigin[]	Indicator.Attribute	Countries Or Regions Of Origin	N/A	Country or region value	One attribute value per country or region.

Microsoft Defender Threat Intel Intel Profile Indicators

The Microsoft Defender Threat Intel Intel Profile Indicators action retrieves indicators associated with the intelligence profile identified by **Related Graph Resource ID** and maps returned indicator details to attributes on the original FQDN or IP indicator. Use the profile's top-level `id` returned by Microsoft Defender Threat Intel Intel Profiles; the submitted indicator value is separate from this field.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/intelProfiles/sample-intel-profile-id/indicators",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type":
"#microsoft.graph.security.intelligenceProfileIndicator",
      "id": "ff3eecd2-a2be-27c2-8dc0-40d1c0eada55",
      "source": "microsoft",
      "firstSeenDateTime": "2022-05-02T23:09:20Z",
      "lastSeenDateTime": null,
      "artifact": {
        "@odata.type": "#microsoft.graph.security.hostname",
        "id": "fake-malicious.site"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.source`	`Indicator.Attribute`	`Source`	`N/A`	`microsoft`	`Source of the related profile indicator.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2022-05-02T23:09:20Z	First observation time when returned.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2022-10-02T23:09:20Z	N/A
.artifact.id	Indicator.Attribute	Artifact ID	N/A	fake-malicious.site	Value of the related artifact.
.id	Indicator.Attribute	ID	N/A	ff3eecd2-a2be-27c2-8dc0-40d1c0eada55	Microsoft Graph ID of the profile indicator.

Microsoft Defender Threat Intel Vulnerability

The Microsoft Defender Threat Intel Vulnerability action retrieves vulnerability intelligence for a CVE indicator and maps available vulnerability details to the original indicator. The description content is cleaned with the shared description formatter and published in the indicator's Description field.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/vulnerabilities/CVE-2021-44228",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.type": "#microsoft.graph.security.vulnerability",
  "id": "CVE-2021-44228",
  "createdDateTime": "2021-11-27T13:18:28.240Z",
  "lastModifiedDateTime": "2023-02-06T18:53:00Z",
  "publishedDateTime": "2021-12-10T18:15:00Z",
  "description": {
    "content": "Apache Log4j2 JNDI features can allow remote code
execution.",
    "format": "markdown"
  },
  "remediation": {
    "content": "Upgrade to a fixed Apache Log4j release.",
    "format": "markdown"
  },
  "severity": "critical",
  "priorityScore": 100,
  "activeExploitsObserved": true,
  "exploitsAvailable": true,
  "hasChatter": true,
  "cvss2Summary": {
    "score": 9.3,
    "severity": "critical",
```

```
    "vectorString": "AV:N/AC:M/Au:N/C:C/I:C/A:C"
  },
  "cvss3Summary": {
    "score": 10.0,
    "severity": "critical",
    "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
  },
  "commonWeaknessEnumerationIds": ["CWE-917"],
  "exploits": [],
  "references": []
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.id	Indicator.Attribute	ID	N/A	CVE-2021-44228	Microsoft Graph vulnerability identifier.
.createdDateTime	Indicator.Attribute	Created Date Time	N/A	2021-11-27T13:18:28.240Z	Record creation time.
.lastModifiedDateTime	Indicator.Attribute	Last Modified Date Time	N/A	2023-02-06T18:53:00Z	Most recent record update time.
.publishedDateTime	Indicator.Attribute	Published Date Time	N/A	2021-12-10T18:15:00Z	Vulnerability publication time.
.severity	Indicator.Attribute	Severity	N/A	critical	Vulnerability severity.
.priorityScore	Indicator.Attribute	Priority Score	N/A	100	Microsoft priority score.
.activeExploitsObserved	Indicator.Attribute	Active Exploits Observed	N/A	true	Indicates whether active exploitation was observed.
.exploitsAvailable	Indicator.Attribute	Exploits Available	N/A	true	Indicates whether exploits are available.
.hasChatter	Indicator.Attribute	Has Chatter	N/A	true	Indicates whether Microsoft reports related chatter.
.description.content	Indicator.Description	Description	N/A	Apache Log4j2 JNDI features can allow remote code execution.	Cleaned with the shared description formatter.
.remediation.content	Indicator.Attribute	Remediation Content	N/A	Upgrade to a fixed Apache Log4j release.	Remediation content.
.cvss2Summary.score	Indicator.Attribute	CVSS 2 Summary Score	N/A	9.3	CVSS v2 score.
.cvss2Summary.severity	Indicator.Attribute	CVSS 2 Summary Severity	N/A	critical	CVSS v2 severity.
.cvss2Summary.vectorString	Indicator.Attribute	CVSS 2 Summary Vector String	N/A	AV:N/AC:M/Au:N/C:C/I:C/A:C	CVSS v2 vector.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.cvss3Summary.score	Indicator.Attribute	CVSS 3 Summary Score	N/A	10.0	CVSS v3 score.
.cvss3Summary.severity	Indicator.Attribute	CVSS 3 Summary Severity	N/A	critical	CVSS v3 severity.
.cvss3Summary.vectorString	Indicator.Attribute	CVSS 3 Summary Vector String	N/A	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	CVSS v3 vector.
.commonWeaknessEnumerationIds[]	Indicator.Attribute	Common Weakness Enumeration Ids	N/A	CWE-917	One attribute value per weakness ID.
.exploits[]	Indicator.Attribute	Exploits	N/A	Exploit identifier or details	One attribute value per exploit; no value is published for an empty list.
.references[]	Indicator.Attribute	References	N/A	Reference URL or details	One attribute value per reference; no value is published for an empty list.

Microsoft Defender Threat Intel Vulnerability Components

The Microsoft Defender Threat Intel Vulnerability Components action retrieves software components associated with a CVE indicator and maps each returned component's ID and name to the original indicator. Each component is processed separately, so the `ID` and `Name` attributes repeat for each component.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/vulnerabilities/CVE-2021-44228/components",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type":
"#microsoft.graph.security.vulnerabilityComponent",
      "id":
"Y3ZlLTIwMjEtNDQyMjg3MTQwOUFwYWNoZSBTb2Z0d2FyZSBGb3VuZGF0aW9uIExvZzRq
IDIuMA==",
      "name": "Apache Software Foundation Log4j 2.0"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.id`	`Indicator.Attribute`	`ID`	`N/A`	`Y3ZlLTIwMjEtNDQyMjg3MTQwOUFwYWNoZSBTb2Z0d2FyZSBGb3VuZGF0aW9uIExvZzRqIDIuMA==`	`Component identifier returned by Microsoft Graph.`
`.name`	`Indicator.Attribute`	`Name`	`N/A`	`Apache Software Foundation Log4j 2.0`	`Component name returned by Microsoft Graph.`

Microsoft Defender Threat Intel Host Port Details

The Microsoft Defender Threat Intel Host Port Details action retrieves one Microsoft Graph hostPort by its resource ID and maps port information, banners, services, the most recent SSL certificate ID, and host ID to the original indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/hostPorts/ODUuMTMuMTM5LjE4JCQ0NDM=",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": {
    "@odata.type": "#microsoft.graph.security.hostPort",
    "id": "ODUuMTMuMTM5LjE4JCQ0NDM=",
    "firstSeenDateTime": "2026-01-10T08:00:00Z",
    "lastScanDateTime": "2026-08-14T10:30:00Z",
    "lastSeenDateTime": "2026-08-14T10:25:00Z",
    "port": 443,
    "protocol": "tcp",
    "status": "open",
    "timesObserved": 42,
    "banners": [
      {
        "banner": "HTTP/1.1 200 OK",
        "firstSeenDateTime": "2026-08-01T10:00:00Z",
        "lastSeenDateTime": "2026-08-14T10:25:00Z",
        "scanProtocol": "https",
        "timesObserved": 4
      }
    ],
    "services": [
      {
        "firstSeenDateTime": "2026-08-01T10:00:00Z",
        "lastSeenDateTime": "2026-08-14T10:25:00Z",
```

```
        "isRecent": true,
        "component": {
          "id": "sample-component-id",
          "name": "Example Server",
          "version": "1.0",
          "category": "Server"
        }
      }
    ],
    "mostRecentSslCertificate": {
      "id": "sample-ssl-certificate-id"
    },
    "host": {
      "id": "example.test"
    }
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.id	Indicator.Attribute	ID	N/A	ODUuMTMuMTM5LjE4JCQ0NDM=	Graph identifier for the host port.
.port	Indicator.Attribute	Port	N/A	443	Port number.
.protocol	Indicator.Attribute	Protocol	N/A	tcp	Protocol used to scan the port.
.status	Indicator.Attribute	Status	N/A	open	Port status.
.timesObserved	Indicator.Attribute	Times Observed	N/A	42	Total observations across scans.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.lastScanDateTime	Indicator.Attribute	Last Scan Date Time	N/A	2026-08-14T10:30:00Z	Most recent scan time.
.banners	Indicator.Attribute	Banners	N/A	Banner object, such as HTTP/1.1 200 OK	Each returned banner is published as a separate value.
.services	Indicator.Attribute	Services	N/A	Service object, such as Example Server	Each returned service is published as a separate value.
.mostRecentSslCertificate.id	Indicator.Attribute	Most Recent SSL Certificate ID	N/A	sample-ssl-certificate-id	ID of the most recent certificate associated with the port.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.host.id	Indicator.Attribute	Host ID	N/A	example.test	Host associated with the port.

Microsoft Defender Threat Intel SSL Certificates

The Microsoft Defender Threat Intel SSL Certificates action searches Microsoft Graph SSL certificates using the submitted indicator as the certificate subject common name.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/sslCertificates?$search=\"subject/
commonName:example.test\"",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.sslCertificate",
      "id": "sample-ssl-certificate-id",
      "expirationDateTime": "2027-08-01T00:00:00Z",
      "fingerprint":
"fb:96:55:15:05:f1:ed:b2:4d:d3:b3:6f:cf:fd:b7:65:83:3b:81:18",
      "firstSeenDateTime": "2026-01-10T08:00:00Z",
      "issueDateTime": "2026-08-01T00:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:25:00Z",
      "serialNumber":
"113738955988571777017519132927338670571909973",
      "sha1": "fb96551505f1edb24dd3b36fcffdb765833b8118",
      "subject": {
        "commonName": "example.test",
        "organizationName": "Example Organization",
        "alternateNames": ["www.example.test"]
      },
      "issuer": {
        "commonName": "Example Issuing CA",
        "organizationName": "Example Certificate Authority"
      }
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.id	Indicator.Attribute	ID	N/A	sample-ssl-certificate-id	Graph certificate identifier.
.fingerprint	Indicator.Attribute	Fingerprint	N/A	fb:96:55:15:05:f1:ed:b2:4d:d3:b3:6f:cf:fd:b7:65:83:3b:81:18	Certificate fingerprint.
.sha1	Indicator.Attribute	SHA1	N/A	fb96551505f1edb24dd3b36fcffdb765833b8118	SHA-1 digest.
.serialNumber	Indicator.Attribute	Serial Number	N/A	113738955988571777017519132927338670571909973	Certificate serial number.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2026-01-10T08:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:25:00Z	Most recent observation time.
.issueDateTime	Indicator.Attribute	Issue Date Time	N/A	2026-08-01T00:00:00Z	Certificate issue time.
.expirationDateTime	Indicator.Attribute	Expiration Date Time	N/A	2027-08-01T00:00:00Z	Certificate expiration time.
.subject.commonName	Indicator.Attribute	Subject Common Name	N/A	example.test	Subject common name.
.subject.organizationName	Indicator.Attribute	Subject Organization Name	N/A	Example Organization	Subject organization.
.subject.alternateNames	Indicator.Attribute	Subject Alternate Name	N/A	www.example.test	One attribute value per alternate name.
.issuer.commonName	Indicator.Attribute	Issuer Common Name	N/A	Example Issuing CA	Issuer common name.
.issuer.organizationName	Indicator.Attribute	Issuer Organization Name	N/A	Example Certificate Authority	Issuer organization.

Microsoft Defender Threat Intel WHOIS Records

The Microsoft Defender Threat Intel WHOIS Records action searches WHOIS records by the nameserver host ID matching the submitted FQDN and maps returned registration data to that indicator.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/whoisRecords?$search=\"nameservers/host/
id:example.test\"",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "value": [
    {
      "@odata.type": "#microsoft.graph.security.whoisRecord",
      "id": "sample-whois-record-id",
      "domainStatus": "client transfer prohibited",
      "expirationDateTime": "2027-01-02T00:00:00Z",
      "firstSeenDateTime": "2020-01-02T00:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:30:00Z",
      "lastUpdateDateTime": "2026-08-14T10:30:00Z",
      "registrationDateTime": "2020-01-02T00:00:00Z",
      "whoisServer": "whois.example.test",
      "registrar": {"name": "Example Registrar"},
      "registrant": {
        "name": "Example Registrant",
        "organization": "Example Organization"
      },
      "nameservers": [
        {
          "firstSeenDateTime": "2020-01-02T00:00:00Z",
          "lastSeenDateTime": "2026-08-14T10:30:00Z",
          "host": {"id": "ns1.example.test"}
        }
```

```
        ]
      }
    ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.domainStatus	Indicator.Attribute	Domain Status	N/A	client transfer prohibited	Status value or values returned for the record.
.registrationDateTime	Indicator.Attribute	Registration Date Time	N/A	2020-01-02T00:00:00Z	Domain registration time.
.expirationDateTime	Indicator.Attribute	Expiration Date Time	N/A	2027-01-02T00:00:00Z	Record expiration time.
.lastUpdateDateTime	Indicator.Attribute	Last Update Date Time	N/A	2026-08-14T10:30:00Z	Last update time.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2020-01-02T00:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:30:00Z	Most recent observation time.
.whoisServer	Indicator.Attribute	WHOIS Server	N/A	whois.example.test	WHOIS server name.
.registrar.name	Indicator.Attribute	Registrar Name	N/A	Example Registrar	Registrar name.
.registrant.name	Indicator.Attribute	Registrant Name	N/A	Example Registrant	Registrant name.
.registrant.organization	Indicator.Attribute	Registrant Organization	N/A	Example Organization	Registrant organization.
.nameservers	Indicator.Attribute	Nameservers	N/A	Nameserver object, such as ns1.example.test	Each returned nameserver is published as a separate value.

Microsoft Defender Threat Intel WHOIS Record Details

The Microsoft Defender Threat Intel WHOIS Record Details action retrieves one WHOIS record by its Microsoft Graph resource ID and maps its details to the original FQDN or IP indicator. Use the record's top-level `id` returned by WHOIS Records.

Sample Request

```
{
  "method": "GET",
  "url": "https://graph.microsoft.com/v1.0/security/
threatIntelligence/whoisRecords/sample-whois-record-id",
  "headers": {
    "Authorization": "Bearer <access_token>"
  }
}
```

Sample Response

```
{
  "@odata.type": "#microsoft.graph.security.whoisRecord",
  "id": "sample-whois-record-id",
  "domainStatus": "client transfer prohibited",
  "expirationDateTime": "2027-01-02T00:00:00Z",
  "firstSeenDateTime": "2020-01-02T00:00:00Z",
  "lastSeenDateTime": "2026-08-14T10:30:00Z",
  "lastUpdateDateTime": "2026-08-14T10:30:00Z",
  "registrationDateTime": "2020-01-02T00:00:00Z",
  "whoisServer": "whois.example.test",
  "registrar": {"name": "Example Registrar"},
  "registrant": {
    "name": "Example Registrant",
    "organization": "Example Organization"
  },
  "admin": {"name": "Example Administrator"},
  "technical": {"name": "Example Technical Contact"},
  "abuse": {"name": "Abuse Contact"},
  "nameservers": [
    {
      "firstSeenDateTime": "2020-01-02T00:00:00Z",
      "lastSeenDateTime": "2026-08-14T10:30:00Z",
      "host": {"id": "ns1.example.test"}
    }
```

```
  ],
  "rawWhoisText": "Example WHOIS text with contact values redacted."
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.domainStatus	Indicator.Attribute	Domain Status	N/A	client transfer prohibited	Status value or values returned for the record.
.registrationDateTime	Indicator.Attribute	Registration Date Time	N/A	2020-01-02T00:00:00Z	Domain registration time.
.expirationDateTime	Indicator.Attribute	Expiration Date Time	N/A	2027-01-02T00:00:00Z	Record expiration time.
.lastUpdateDateTime	Indicator.Attribute	Last Update Date Time	N/A	2026-08-14T10:30:00Z	Last update time.
.firstSeenDateTime	Indicator.Attribute	First Seen Date Time	N/A	2020-01-02T00:00:00Z	First observation time.
.lastSeenDateTime	Indicator.Attribute	Last Seen Date Time	N/A	2026-08-14T10:30:00Z	Most recent observation time.
.whoisServer	Indicator.Attribute	WHOIS Server	N/A	whois.example.test	WHOIS server name.
.registrar.name	Indicator.Attribute	Registrar Name	N/A	Example Registrar	Registrar name.
.registrant.name	Indicator.Attribute	Registrant Name	N/A	Example Registrant	Registrant name.
.registrant.organization	Indicator.Attribute	Registrant Organization	N/A	Example Organization	Registrant organization.
.admin.name	Indicator.Attribute	Admin Name	N/A	Example Administrator	Administrative contact name.
.technical.name	Indicator.Attribute	Technical Name	N/A	Example Technical Contact	Technical contact name.
.abuse.name	Indicator.Attribute	Abuse Name	N/A	Abuse Contact	Abuse contact name.
.nameservers	Indicator.Attribute	Nameservers	N/A	Nameserver object, such as ns1.example.test	Each returned nameserver is published as a separate value.
.rawWhoisText	Indicator.Attribute	Raw WHOIS Text	N/A	WHOIS text with contact values redacted	Raw WHOIS text returned by Microsoft Graph.

Enriched Data

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

Microsoft Defender Threat Intel Host Details

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	4

Microsoft Defender Threat Intel Host Reputation

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	6

Microsoft Defender Threat Intel WHOIS Lookup

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	8

Microsoft Defender Threat Intel WHOIS History

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	11

Microsoft Defender Threat Intel Forward Passive DNS

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	6

Microsoft Defender Threat Intel Reverse Passive DNS

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	6

Microsoft Defender Threat Intel Host Cookies

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	4

Microsoft Defender Threat Intel Host Components

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	5

Microsoft Defender Threat Intel Host Pairs

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	5

Microsoft Defender Threat Intel Parent Host Pairs

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	5

Microsoft Defender Threat Intel Child Host Pairs

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	5

Microsoft Defender Threat Intel Host Ports

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	2
Indicator Attributes	9

Microsoft Defender Threat Intel Host SSL Certificates

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	9

Microsoft Defender Threat Intel Host Trackers

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	4

Microsoft Defender Threat Intel Subdomains

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	2

Microsoft Defender Threat Intel Articles

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	8

Microsoft Defender Threat Intel Article Details

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	8

Microsoft Defender Threat Intel Article Indicators

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	3

Microsoft Defender Threat Intel Intel Profiles

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	10

Microsoft Defender Threat Intel Intel Profile Details

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	10

Microsoft Defender Threat Intel Intel Profile Indicators

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	5

Microsoft Defender Threat Intel Vulnerability

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	15

Microsoft Defender Threat Intel Vulnerability Components

METRIC	RESULT
Run Time	2 minutes
Indicators	2
Indicator Attributes	4

Microsoft Defender Threat Intel Host Port Details

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	2
Indicator Attributes	24

Microsoft Defender Threat Intel SSL Certificates

METRIC	RESULT
Run Time	2 minutes
Indicators	3
Indicator Attributes	39

Microsoft Defender Threat Intel WHOIS Records

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	11

Microsoft Defender Threat Intel WHOIS Record Details

METRIC	RESULT
Run Time	2 minutes

METRIC	RESULT
Indicators	1
Indicator Attributes	12

Known Issues / Limitations

- The API can return `402 Payment Required` if the tenant is not entitled to the Microsoft Defender Threat Intelligence API.
- A `401` or `403` response indicates that credentials, admin consent, `ThreatIntelligence.Read.All`, or tenant entitlement should be checked.

Change Log

- **Version 1.0.0**
  - Initial release