ThreatQuotient

IBM X-Force Exchange Action Bundle

Version 1.0.0

April 22, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email:	support@threatq.com
Web:	support.threatq.com
Phone:	703.574.9893

Contents

Warning and Disclaimer

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

Support

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

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

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

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

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

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The IBM X-Force Exchange Action Bundle enables the automatic enrichment of indicators within your Threat Library.

The integrations provides the following actions:

- **IBM X-Force Exchange Enrichment -** fetches enrichment context such as tags, categories, and scores from the IBM X-Force Exchange API.
- **IBM X-Force Exchange - Get Relation IOCs -** fetches indicators associated with malware that are related to the input indicators.

The actions are compatible with the following indicator types:

- CVE
- FQDN
- IP Address
- IPv6 Address
- URL
- MD5
- SHA-1
- SHA-256

The actions return enriched indicators to the ThreatQ platform.

> 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 at least one of the following indicator types:
    - CVE
    - FQDN
    - IP Address
    - IPv6 Address
    - URL
    - MD5
    - SHA-1
    - SHA-256

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
6. Select the actions to install, when prompted, and click on **Install**.

    > 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(s).

Configuration

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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **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:

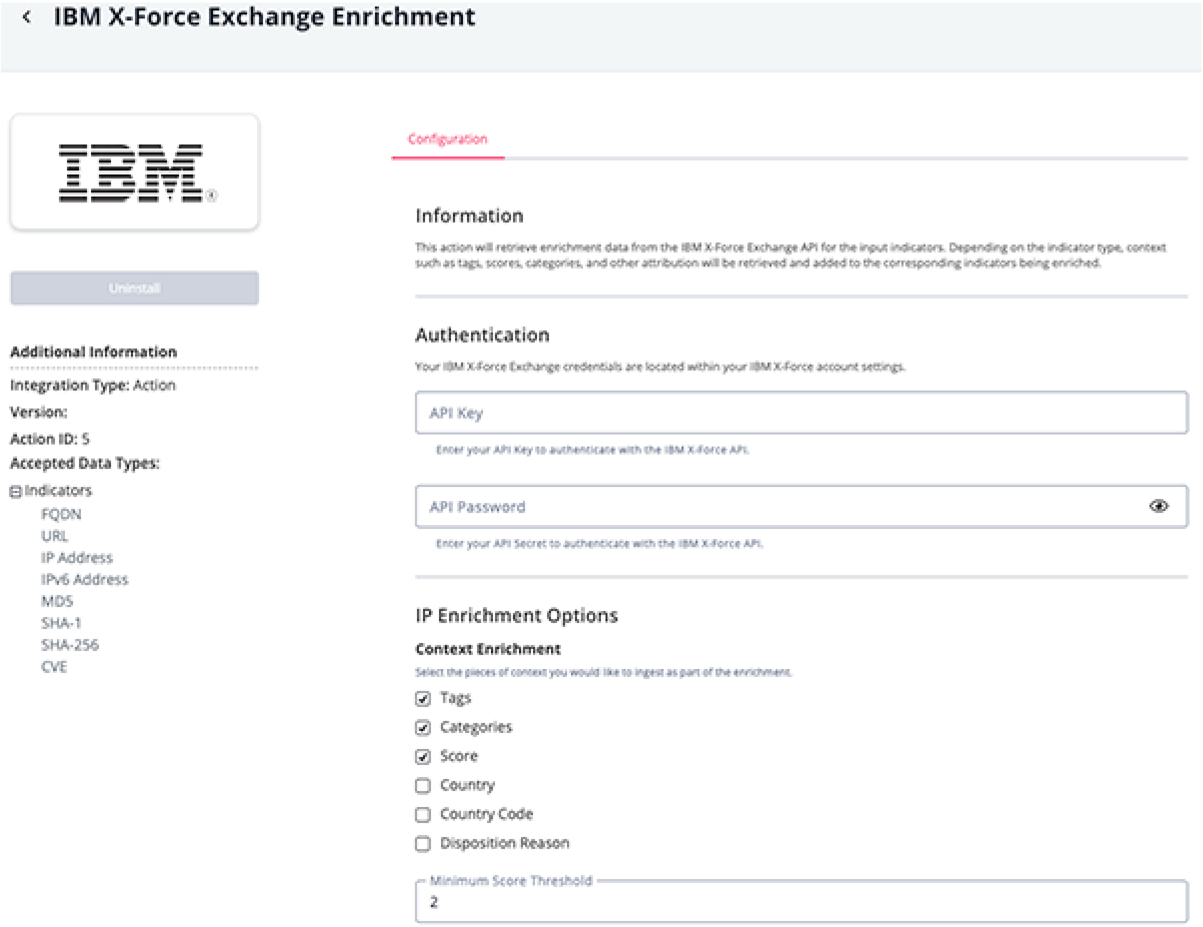
> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's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

IBM X-Force Exchange Enrichment Parameters

PARAMETER	DESCRIPTION
Authentication	
API Key	Enter your OAuth Client ID to authenticate with the ThreatVision API.
API Password	Enter your API Secret to authenticate with the IBM X-Force API.
IP Enrichment Options	
Context Enrichment	Select the pieces of context to ingest as part of the enrichment. Options include: ◦ Tags (default) ◦ Categories (default) ◦ Score (default) ◦ Country ◦ Country Code ◦ Disposition Reason

PARAMETER	DESCRIPTION
Minimum Score Threshold	Only ingest enrichment for indicators with a score greater than or equal to this value. Typically, uncategorized indicators will be scored a 1. The default value is 2.
Include Category Percentages	Include the percentage of each category in the enrichment. This option is disabled by default.
File Hash Enrichment Options	
Context Enrichment	Select the pieces of context you would like to ingest as part of the enrichment. Options include: ◦ Tags (default) ◦ Risk (default) ◦ Malware Type (default) ◦ Malware Family (Attribute) (default) ◦ MIME Type ◦ Platform ◦ Community Coverage ◦ Last Seen ◦ First Seen
Relationship Enrichment	Select the relationships you would like to ingest as part of the enrichment. Options include: ◦ Command and Control Domains (default) ◦ Command and Control IPs (default) ◦ Command and Control URLs (default) ◦ Download Server Domains ◦ Download Server IPs ◦ Download Server URLs
Risk Filter	Only ingest enrichment for indicators with a risk within the selected values. Options include: ◦ High (default) ◦ Medium (default) ◦ Low
URL & FQDN Enrichment Options	

PARAMETER	DESCRIPTION
Context Enrichment	Select the pieces of context to ingest as part of the enrichment. Options include: ◦ Tags (default) ◦ Categories (default) ◦ Score (default) ◦ Associated Application
Minimum Score Threshold	Only ingest enrichment for indicators with a score greater than or equal to this value. The default value is 1.
CVE Enrichment Options	
Context Enrichment	Select the pieces of context to ingest as part of the enrichment. Options include: ◦ Score (default) ◦ Vulnerability Title (default) ◦ Description (default) ◦ Affected Platforms (default) ◦ Temporal Score ◦ Remedy ◦ Consequences ◦ Exploitability ◦ External References ◦ Report Confidence
CVSS Enrichment	Select the pieces of CVSS context to ingest as part of the enrichment. Options include: ◦ Privileges Required ◦ User Interaction ◦ Access Vector ◦ Access Complexity ◦ Integrity Impact ◦ Availability Impact ◦ Remediation Level
Minimum Score Threshold	Only ingest enrichment for CVEs with a score greater than or equal to this value. The default value is 5.
Workflow Options	
Objects Per Run	The number of objects to process per run of the workflow. The default value is 1000.



IBM X-Force Exchange Enrichment

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

⊟ Indicators

FQDN

URL

IP Address

IPv6 Address

MD5

SHA-1

SHA-256

CVE

Information

This action will retrieve enrichment data from the IBM X-Force Exchange API for the input indicators. Depending on the indicator type, context such as tags, scores, categories, and other attribution will be retrieved and added to the corresponding indicators being enriched.

Authentication

Your IBM X-Force Exchange credentials are located within your IBM X-Force account settings.

API Key

Enter your API Key to authenticate with the IBM X-Force API.

API Password

Enter your API Secret to authenticate with the IBM X-Force API.

IP Enrichment Options

Context Enrichment

Select the pieces of context you would like to ingest as part of the enrichment.

☑ Tags

☑ Categories

☑ Score

□ Country

□ Country Code

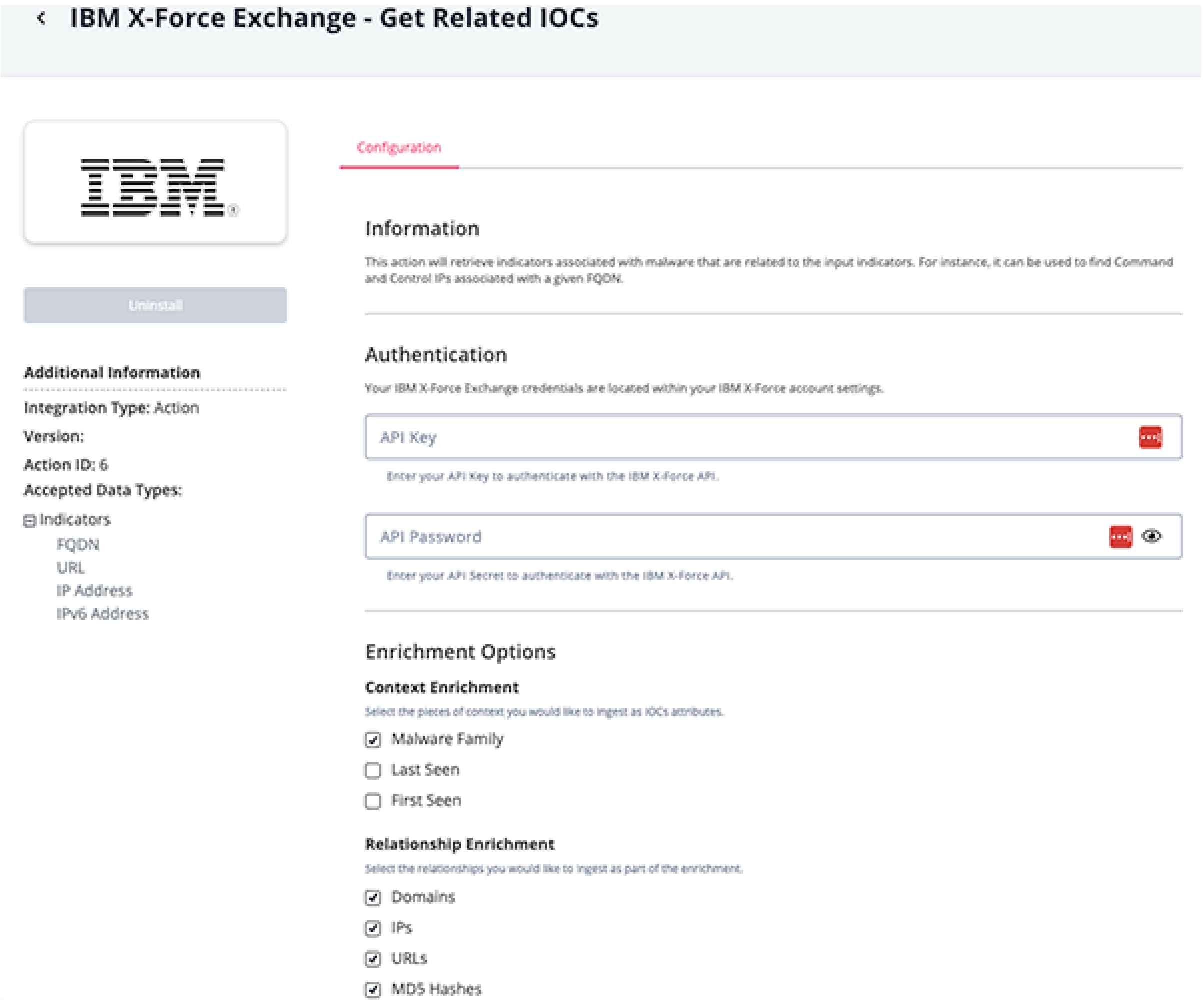
□ Disposition Reason

Minimum Score Threshold: 2

IBM X-Force Exchange Get Related IOCs Parameters

PARAMETER	DESCRIPTION
Authentication	
API Key	Enter your OAuth Client ID to authenticate with the ThreatVision API.
API Password	Enter your API Secret to authenticate with the IBM X-Force API.
Enrichment Options	
Context Enrichment	Select the pieces of context to ingest as part of the enrichment. Options include:

PARAMETER	DESCRIPTION
	◦ Malware Family ◦ Last Seen ◦ First Seen
Relationship Enrichment	Select the relationships to ingest as part of the enrichment. Options include: ◦ Domains (default) ◦ IPs (default) ◦ URLs (default) ◦ MD5 Hashes (default)
WHOIS Enrichment	Select whether or not to ingest WHOIS information as part of the enrichment.
Workflow Options	
Objects Per Run	The number of objects to process per run of the workflow. The default value is 1000.



Additional Information

Integration Type: Action

Version:

Action ID: 6

Accepted Data Types:

⊟ Indicators
- FQDN
- URL
- IP Address
- IPv6 Address

Information

This action will retrieve indicators associated with malware that are related to the input indicators. For instance, it can be used to find Command and Control IPs associated with a given FQDN.

Authentication

Your IBM X-Force Exchange credentials are located within your IBM X-Force account settings.

API Key

Enter your API Key to authenticate with the IBM X-Force API.

API Password

Enter your API Secret to authenticate with the IBM X-Force API.

Enrichment Options

Context Enrichment

Select the pieces of context you would like to ingest as IOCs attributes.

☑ Malware Family

☐ Last Seen

☐ First Seen

Relationship Enrichment

Select the relationships you would like to ingest as part of the enrichment.

☑ Domains

☑ IPs

☑ URLs

☑ MD5 Hashes

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
IBM X-Force Exchange Enrichment	This action will retrieve enrichment data from the IBM X-Force Exchange API for the input indicators.	Indicators	IP Address, FQDN, URL, MD5, SHA-1, SHA-256, CVE
IBM X-Force Exchange - Get Related IOCs	This action will retrieve indicators associated with malware that are related to the input indicators.	Indicators	IP Address, FQDN, URL

IBM X-Force Exchange Enrichment

The IBM X-Force Exchange Enrichment action retrieves enrichment data from the IBM X-Force Exchange API for the input indicators. Depending on the indicator type, context such as tags, scores, categories, and other attribution will be retrieved and added to the corresponding indicators being enriched.

See the mapping tables below for specific indicator types.

IP Addresses

`GET https://api.xforce.ibmcloud.com/ipr/{{ value }}`

Sample Response:

```
{
  "ip": "209.197.3.8",
  "history": [
    {
      "created": "2012-03-22T07:26:00.000Z",
      "reason": "Regional Internet Registry",
      "geo": {
        "country": "United States",
        "countrycode": "US"
      },
      "ip": "209.197.0.0/19",
      "categoryDescriptions": {},
      "reasonDescription": "One of the five RIRs announced a (new) location
mapping of the IP.",
      "score": 1,
      "cats": {}
    }
  ],
  "subnets": [
    {
      "created": "2012-03-22T07:26:00.000Z",
      "reason": "Regional Internet Registry",
      "geo": {
        "country": "United States",
        "countrycode": "US"
      },
      "ip": "209.197.0.0",
      "categoryDescriptions": {},
      "reasonDescription": "One of the five RIRs announced a (new) location
mapping of the IP.",
      "score": 1,
      "cats": {},
      "subnet": "209.197.0.0/19"
    }
  ],
  "cats": {
    "Scanning IPs": 43
  },
  "geo": {
    "country": "United States",
    "countrycode": "US"
  },
  "score": 4.3,
  "reason": "Security analyst review",
  "reasonDescription": "Based on the review of an X-Force security analyst.",
  "categoryDescriptions": {
    "Scanning IPs": "These IPs have been identified as illegally scanning
networks for vulnerabilities."
  },
  "tags": []
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.tags[]`	Indicator.Tag	N/A	N/A	N/A	N/A
`.cats[]`	Indicator.Attribute	Category	N/A	`Scanning IPs`	N/A
`.score`	Indicator.Attribute	Score	N/A	`4.3`	Updated at ingestion.
`.geo.country`	Indicator.Attribute	Country	N/A	`United States`	N/A
`.geo.countrycode`	Indicator.Attribute	Country Code	N/A	`US`	N/A
`.reasonDescription`	Indicator.Attribute	Disposition Reason	N/A	`Based on the review of an X-Force security analyst.`	N/A

FQDNs & URLs

`GET https://api.xforce.ibmcloud.com/url/{{ value }}`

Sample Response:

```
{
  "result": {
    "url": "pnc-bankwu.com",
    "cats": {
      "Early Warning": true
    },
    "score": 10,
    "categoryDescriptions": {
      "Early Warning": "This category contains potentially malicious domains
identified by analysing DNS traffic."
    }
  },
  "tags": []
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.tags[]`	Indicator.Tag	N/A	N/A	N/A	N/A
`.result.cats[]`	Indicator.Attribute	Category	N/A	`Spam URLs`	N/A
`.result.score`	Indicator.Attribute	Score	N/A	`9`	Updated at ingestion.
`.result.application.name`	Indicator.Attribute	Associated Application	N/A	N/A	N/A

MD5, SHA-1, and SHA-256 Hashes

`GET https://api.xforce.ibmcloud.com/malware/{{ value }}`

Sample Response:

```
{
  "malware": {
    "origins": {
      "emails": {},
      "CnCServers": {
        "rows": [
          {
            "type": "CnC",
            "md5": "474B9CCF5AB9D72CA8A333889BBB34F0",
            "domain": "pc-guard.net",
            "firstseen": "2014-10-20T23:19:00Z",
            "lastseen": "2014-10-20T23:19:00Z",
            "ip": "61.255.239.86",
            "count": 483,
            "schema": "http",
            "filepath": "v.html",
            "origin": "CnC",
            "uri": "http://pc-guard.net/v.html"
          }
        ],
        "count": 1
      },
      "downloadServers": {},
      "subjects": {},
      "external": {
        "detectionCoverage": 44,
        "family": ["heuristic", "trojan"]
      }
    },
    "type": "md5",
    "md5": "0x474B9CCF5AB9D72CA8A333889BBB34F0",
    "hash": "0x474B9CCF5AB9D72CA8A333889BBB34F0",
    "created": "2014-10-20T23:19:00Z",
    "family": ["tsunami"],
    "familyMembers": {
      "tsunami": {
        "count": 61
      }
    },
    "risk": "high"
  },
  "tags": []
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.tags[]`	Indicator.Tag	N/A	N/A	N/A	N/A
`.malware.risk`	Indicator.Attribute	Risk	N/A	`High`	Updated at ingestion.
`.malware.origins.external.family`	Indicator.Attribute	Malware Family	N/A	`emotet`	N/A
`.malware.family`	Indicator.Attribute	Malware Family	N/A	`emotet`	N/A
`.malware.origins.external.malwareType`	Indicator.Attribute	Malware Type	N/A	`Trojan`	N/A
`.malware.mimetype`	Indicator.Attribute	MIME Type	N/A	`exe`	N/A
`.malware.origins.external.platform`	Indicator.Attribute	Platform	N/A	`Linux`	N/A
`.malware.origins.external.detectionCoverage`	Indicator.Attribute	Community Coverage	N/A	`51%`	Updated at ingestion.
`.malware.origins.external.lastSeen`	Indicator.Attribute	Last Seen	N/A	`2022-03-21T 05:12:34`	Updated at ingestion.
`.malware.origins.external.firstSeen`	Indicator.Attribute	First Seen	N/A	`2022-01-26T 01:15:01`	N/A
`.malware.origins.CnCServers.rows[].ip`	Indicator.Indicator	IP Address or IPv6 Address	N/A	N/A	Added with a `Threat Type: C2` attribute
`.malware.origins.CnCServers.rows[].uri`	Indicator.Indicator	URL	N/A	N/A	Added with a `Threat Type: C2` attribute
`.malware.origins.CnCServers.rows[].domain`	Indicator.Indicator	FQDN	N/A	N/A	Added with a `Threat Type: C2` attribute
`.malware.origins.DownloadServers.rows[].ip`	Indicator.Indicator	IP Address or IPv6 Address	N/A	N/A	Added with a `Threat Type: Download Server` attribute
`.malware.origins.DownloadServers.rows[].domain`	Indicator.Indicator	FQDN	N/A	N/A	Added with a `Threat Type: Download Server` attribute
`.malware.origins.DownloadServers.rows[].uri`	Indicator.Indicator	URL	N/A	N/A	Added with a `Threat Type: Download Server` attribute

CVEs

`GET https://api.xforce.ibmcloud.com/vulnerabilities/search/{{ value }}`

Sample Response:

```
[
  {
    "type": "vulnerability",
    "xfdbid": 260217,
    "updateid": 171362,
    "updated": true,
    "variant": "single",
    "title": "Microsoft Windows and Microsoft Office code execution",
    "description": "Microsoft Windows and Microsoft Office could allow a remote
attacker to execute arbitrary code on the system. By persuading a victim to
open a specially crafted file, an attacker could exploit this vulnerability to
execute arbitrary code on the system.",
    "risk_level": 8.3,
    "cvss": {
      "version": "3.0",
      "privilegesrequired": "None",
      "userinteraction": "Required",
      "scope": "Changed",
      "access_vector": "Network",
      "access_complexity": "High",
      "confidentiality_impact": "High",
      "integrity_impact": "High",
      "availability_impact": "High",
      "remediation_level": "Unavailable"
    },
    "temporal_score": 7.6,
    "remedy": "No remedy available as of July 11, 2023.",
    "remedy_fmt": "<p>No remedy available as of July 11, 2023.</p>",
    "reported": "2023-07-11T00:00:00Z",
    "tagname": "ms-windows-cve202336884-code-exec",
    "stdcode": ["CVE-2023-36884"],
    "platforms_affected": [
      "Microsoft Windows Server 2012",
      "Microsoft Windows Server 2012 R2"
    ],
    "exploitability": "Unproven",
    "consequences": "Gain Access",
    "references": [
      {
        "link_target": "https://msrc.microsoft.com/update-guide/vulnerability/
CVE-2023-36884",
        "link_name": "Microsoft Security TechCenter - July 2023",
        "description": "Office and Windows HTML Remote Code Execution
Vulnerability"
```

```
      }
    ],
    "report_confidence": "Confirmed",
    "uuid": "c31817e6ac25a2cd1598e8be5f3a1444"
  }
]
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.risk_level`	Indicator.Attribute	Score	N/A	`5.8`	Updated at ingestion.
`.title`	Indicator.Attribute	Vulnerability Title	N/A	`Microsoft Windows and Microsoft Office code execution`	N/A
`.description`	Indicator.Attribute	Description	N/A	N.A	N/A
`.platforms_affected[]`	Indicator.Attribute	Affected Platform	N/A	`Microsoft Windows Server 2012`	N/A
`.temporal_score`	Indicator.Attribute	Temporal Score	N/A	`7.6`	N/A
`.remedy`	Indicator.Attribute	Remedy	N/A	`No remedy available as of July 11, 2023.`	N/A
`.consequences`	Indicator.Attribute	Consequences	N/A	`Gain Access`	N/A
`.exploitability`	Indicator.Attribute	Exploitability	N/A	`Unproven`	N/A
`.external_references[].link_target`	Indicator.Attribute	External References	N/A	N/A	N/A
`.report_confidence`	Indicator.Attribute	Report Confidence	N/A	`Confirmed`	N/A
`.cvss.privileges_required`	Indicator.Attribute	Privileges Required	N/A	`None`	N/A
`.cvss.user_interaction`	Indicator.Attribute	User Interaction	N/A	`Required`	N/A
`.cvss.access_vector`	Indicator.Attribute	Access Vector	N/A	`Network`	N/A
`.cvss.access_complexity`	Indicator.Attribute	Access Complexity	N/A	`High`	N/A
`.cvss.integrity_impact`	Indicator.Attribute	Integrity Impact	N/A	`High`	N/A
`.cvss.availability_impact`	Indicator.Attribute	Availability Impact	N/A	`High`	N/A
`.cvss.remediation_level`	Indicator.Attribute	Remediation Level	N/A	`Unavailable`	N/A

IBM X-Force Exchange - Get Related IOCs

The IBM X-Force Exchange - Get Related IOCs action will retrieve indicators associated with malware that are related to the input indicators. For instance, it can be used to find Command and Control IPs associated with a given FQDN.

`GET https://api.xforce.ibmcloud.com/{{ type }}/malware/{{ value }}`

Sample Response:

```
{
  "malware": [
    {
      "type": "WEB",
      "md5": "6865D47EEB5B85D949BDF5BD1BA27AC0",
      "domain": "160.16.58.163",
      "firstseen": "2022-03-31T22:25:00Z",
      "lastseen": "2022-03-31T22:25:00Z",
      "ip": "0x00000000000000000000ffffa0103aa3",
      "count": 1,
      "schema": "http",
      "filepath": "wp-content/.b/pty5",
      "uri": "http://160.16.58.163/wp-content/.b/pty5",
      "first": "2022-03-31T22:25:00Z",
      "last": "2022-03-31T22:25:00Z",
      "origin": "WEB",
      "family": ["gafgyt"]
    },
    {
      "type": "WEB",
      "md5": "582A434BA0F2E04BD8B5495C50320068",
      "domain": "160.16.58.163",
      "firstseen": "2022-03-31T22:25:00Z",
      "lastseen": "2022-03-31T22:25:00Z",
      "ip": "0x00000000000000000000ffffa0103aa3",
      "count": 1,
      "schema": "http",
      "filepath": "wp-content/.b/pty3",
      "uri": "http://160.16.58.163/wp-content/.b/pty3",
      "first": "2022-03-31T22:25:00Z",
      "last": "2022-03-31T22:25:00Z",
      "origin": "WEB",
      "family": ["gafgyt"]
    }
  ]
}
```

`GET https://api.xforce.ibmcloud.com/whois/{{ value }}`

Sample Response:

```
{
    "updatedDate": "2024-04-05T18:43:01.000Z",
    "contactEmail": "hm-changed@vnnic.vn",
    "registrarName": "APNIC",
    "netRange": "116.96.0.0 - 116.111.255.255",
    "contact": [
        {
            "type": "registrant",
            "name": "Viettel Group",
            "organization": "VIETTEL-VN",
            "country": "Vietnam"
        }
    ],
    "extended": {
        "updatedDate": "2024-04-05T18:43:01.000Z",
        "contactEmail": "hm-changed@vnnic.vn",
        "registrarName": "APNIC",
        "netRange": "116.96.0.0 - 116.111.255.255",
        "contact": [
            {
                "type": "registrant",
                "name": "Viettel Group",
                "organization": "VIETTEL-VN",
                "country": "Vietnam"
            }
        ]
    }
}
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.malware[].domain`	Related Indicator	FQDN	N/A	N/A	N/A
`.malware[].ip`	Related Indicator	IP Address or IPv6 Address	N/A	N/A	N/A
`malware[].uri`	Related Indicator	URL	N/A	N/A	N/A
`.malware[].md5`	Related Indicator	MD5	N/A	N/A	N/A
`.malware[].type`	Indicator Attribute	Malware Type	N/A	`WEB`	Updated at ingestion.
`.malware[].family[]`	Related Indicator Attribute	Malware Family	N/A	`tsunami`	N/A
`.malware[].lastseen`	Related Indicator Attribute	Last Seen	N/A	`2022-03-31T22:25:00Z`	If 'Last Seen' user fields is selected. Updated at ingestion.
`.malware[].firstseen`	Related Indicator Attribute	First Seen	N/A	`2022-03-31T22:25:00Z`	If 'First Seen' user fields is selected
`.whois.contactEmail`	Related Indicator	Email Address	N/A	`hm-changed@vnnic.vn`	If 'WHOIS' user fields is selected
`.whois.registrarName`	Related Indicator Attribute	Registrar Name	N/A	`APNIC`	If 'WHOIS' user fields is selected
`.whois.contact.country`	Indicator Attribute	Country	N/A	`Vietnam`	If 'WHOIS' user fields is selected
`.whois.contact.type`	Indicator Attribute	Type	N/A	`registrant`	If 'WHOIS' user fields is selected
`.whois.contact. organization`	Indicator Attribute	Organization	N/A	`VIETTEL-VN`	If 'WHOIS' user fields is selected
`.whois.createdDate`	Indicator Attribute	Created Date	N/A	N/A	If 'WHOIS' user fields is selected
`.whois.updatedDate`	Indicator Attribute	Updated Date	N/A	`024-04-05T18:43:01.000Z`	If 'WHOIS' user fields is selected. Updated at ingestion.

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.

IBM X-Force Exchange Enrichment

METRIC	RESULT
Run Time	4 minutes
Indicators	266
Indicator Attributes	538

IBM X-Force Exchange Get Related IOCs

METRIC	RESULT
Run Time	1 minute
Indicators	102
Indicator Attributes	304

Known Issues / Limitations

- You will be limited to your IBM X-Force Exchange API rate limit.   Be aware of this rate limit and use the **Objects Per Run** parameter configuration accordingly.
- Related indicators are limited to a maximum number of 200.

Change Log

- **Version 1.0.0**
  - Initial release