ThreatQuotient

IBM X-Force Exchange Operation User Guide

Version 1.1.1

October 28, 2023

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	1.1.1
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

IBM X-Force Exchange is a cloud-based threat intelligence platform that allows you to consume, share and act on threat intelligence. It enables you to rapidly research the latest global security threats, aggregate actionable intelligence, consult with experts and collaborate with peers. IBM X-Force Exchange, supported by human- and machine-generated intelligence, leverages the scale of IBM X-Force to help users stay ahead of emerging threats.

The IBM X-Force Exchange operation provides Data Enrichment of indicators of compromise via the X-Force Exchange.

The operation provides the following actions:

- **IP Report** - provides a summary of reputation information about an IP address.
- **Malware For IP** - looks up malware associated with an IP Address.
- **URL Report** - provides a summary of reputation information about a URL or FQDN.
- **Malware for URL** - provides Malware listings associated with a URL or FQDN.
- **Malware for File Hash** - provides a summary reputation report for MD5, SHA1, SHA256.
- **Vulnerability Report** - returns information about a CVE.
- **WHOIS** - returns WHOIS information for an IP or FQDN.

The operation is compatible with the following indicator types:

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

Installation

Perform the following steps to install the integration:

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

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

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your X-Force Exchange API Key to be used in HTTP headers for accessing feed data.
API Password	Your X-Force Exchange API Password to be used in HTTP headers for accessing feed data.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
IP Report	Provides a summary of reputation information about an IP address.	Indicator	IP Address
Malware For IP	Looks up malware associated with an IP Address.	Indicator	IP Address
URL Report	Provides a summary of reputation information about a URL or FQDN.	Indicator	URL, FQDN
Malware For URL	Provides Malware listings associated with a URL or FQDN.	Indicator	URL, FQDN
Malware for File Hash	Provides a summary reputation report for MD5, SHA1, SHA256.	Indicator	MD5, SHA1, SHA256
Vulnerability Report	Returns information about a CVE.	Indicator	CVE
WHOIS	Returns WHOIS information for an IP or FQDN.	Indicator	IP Address, FQDN

IP Report

The IP Report action provides a summary of reputation information about an IP address.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.geo.countrycode	Indicator.Attribute	Country Code	US	N/A
.geo.country	Indicator.Attribute	Country	United States	N/A
.reason	Indicator.Attribute	X-Force Reason	One of the five RIRs announced a (new) location mapping of the IP.	N/A
.score	Indicator.Attribute	X-Force Score	1	N/A
.cats	Indicator.Attribute	X-Force Exchange Category	N/A	Extracted from the mapping's keys
.tags[].date	Indicator.Attribute	Date of Report	N/A	N/A
.subnets[].subnet	RelatedIndicator.Value	CIDR Block	8.8.8.0/24	N/A
.subnets[].score	RelatedIndicator.Attribute	X-Force Exchange Score	1	N/A
.subnets[].geo.countrycode	RelatedIndicator.Attribute	Country Code	US	N/A
.subnets[].geo.country	RelatedIndicator.Attribute	Country	United States	N/A

Malware for IP

The Malware for IP action looks up malware associated with an IP Address.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.malware[].family	Indicator.Attribute	Malware Family	Spam Zero-Day	N/A
.malware[].domain	RelatedIndicator.Value	FQDN	soneramail.nl	N/A
.malware[].md5	RelatedIndicator.Value	MD5	256001D33DA5A13B1AD2E2322CE0B19E	N/A
.malware[].firstseen	RelatedIndicator.Attribute	First Seen Date	2015-10-26T16:15:00Z	N/A

URL Report

The URL Report action provides a summary of reputation information about a URL or FQDN.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.score	Indicator.Attribute	X-Force Exchange Score	1	N/A
.result.cats	Indicator.Attribute	X-Force Exchange Category	Software / Hardware	Extracted from the mapping's keys
.result.application.riskfactors	Indicator.Attribute	Risk Factor	Insecure communication	Extracted from the mapping's keys
.result.application.name	Indicator.Attribute	Application Name	IBM Kenexa CompAnalyst	N/A
.result.application.urls	RelatedIndicator.Value	URL	https://ibm.com	N/A
.result.application.urls	RelatedIndicator.Value	FQDN	ibm.com	N/A
.result.application.baseurl	RelatedIndicator.Value	URL	http://01.ibm.com/software/smarterworkforce/compensation_divestiture	N/A

Malware for URL

The Malware for URL action provides Malware listings associated with a URL or FQDN.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.malware[].type	Indicator.Attribute	Malware Type	SPM	N/A
.malware[].md5	RelatedIndicator.Value	MD5	3018E99857F31A59E0777396AE634A8F	N/A
.malware[].domain	RelatedIndicator.Value	FQDN	ibm.com	N/A
.malware[].uri	RelatedIndicator.Value	URL	34835856.zip	N/A
.malware[].ip	RelatedIndicator.Value	IP Address	87.235.177.251	N/A

Malware for File Hash

The Malware for File Hash action provides a summary reputation report for MD5, SHA1, SHA256.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.malware.created	Indicator.Attribute	Created Date	2014-10-20T23:19:00Z	N/A
.malware.risk	Indicator.Attribute	Risk	high	N/A
.malware.origins.external.family	Indicator.Attribute	Malware Family	generic	N/A
.malware.family	Indicator.Attribute	Malware Family	tsunami	N/A
.malware.origins.CnCServers.rows.md5	RelatedIndicator.Value	MD5	3018E99857F31A59E07 77396AE634A8F	Added with attribute `Origin = CnCServers`
.malware.origins.CnCServers.rows.domain	RelatedIndicator.Value	FQDN	pc-guard.net	Added with attribute `Origin = CnCServers`
.malware.origins.CnCServers.rows.ip	RelatedIndicator.Value	IP Address	61.255.239.86	Added with attribute `Origin = CnCServers`
.malware.origins.CnCServers.rows.uri	RelatedIndicator.Value	URL	http://pc-guard.net/ v.html	Added with attribute `Origin = CnCServers`
.malware.origins.downloadServers.rows.md5	RelatedIndicator.Value	MD5	3018E99857F31A59E07 77396AE634A8F	Added with attribute `Origin = Download Servers`
.malware.origins.downloadServers.rows.domain	RelatedIndicator.Value	FQDN	pc-guard.net	Added with attribute `Origin = Download Servers`
.malware.origins.downloadServers.rows.ip	RelatedIndicator.Value	IP Address	61.255.239.86	Added with attribute `Origin = Download Servers`
.malware.origins.downloadServers.rows.uri	RelatedIndicator.Value	URL	http://pc-guard.net/ v.html	Added with attribute `Origin = Download Servers`
.malware.origins.emails.rows.md5	RelatedIndicator.Value	MD5	3018E99857F31A59E07 77396AE634A8F	Added with attribute `Origin = Email`
.malware.origins.emails.rows.domain	RelatedIndicator.Value	FQDN	pc-guard.net	Added with attribute `Origin = Email`
.malware.origins.emails.rows.ip	RelatedIndicator.Value	IP Address	61.255.239.86	Added with attribute `Origin = Email`
.malware.origins.emails.rows.uri	RelatedIndicator.Value	URL	http://pc-guard.net/ v.html	Added with attribute `Origin = Email`
.malware.origins.subjects.rows.md5	RelatedIndicator.Value	MD5	3018E99857F31A59E077 7396AE634A8F	Added with attribute `Origin = Subject`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.malware.origins.subjects.rows.domain	RelatedIndicator.Value	FQDN	pc-guard.net	Added with attribute `Origin = Subject`
.malware.origins.subjects.rows.ip	RelatedIndicator.Value	IP Address	61.255.239.86	Added with attribute `Origin = Subject`
.malware.origins.subjects.rows.uri	RelatedIndicator.Value	URL	http://pc-guard.net/v.html	Added with attribute `Origin = Subject`

Vulnerability Report

The Vulnerability Report action returns information about a CVE.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.[].values()	Indicator.Attribute	[].keys()	Denial of Service	The Attribute Key is the value that it's on '[].keys()'. Ex: Consequences
.[].cvss.values()	Indicator.Attribute	CVSS + []cvss.keys()	Low	The Attribute Key is 'CVSS' appending the value that it's on '[]cvss.keys()'. Ex: CVSS Access Complexity
.[].platforms_affected[]	Indicator.Attribute	Platforms Affected	HP Integrated Lights-Out 2 (iLO2) 2.23	N/A
.[].references[].link_target	Indicator.Attribute	Vulnerability Link	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2601	N/A

WHOIS

The WHOIS action returns WHOIS information for an IP or FQDN.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
extended.createdDate	Indicator.Attribute	Created Date	1986-03-19T00:00:00.000Z	N/A
.extended.expiresDate	Indicator.Attribute	Expires Date	2021-03-20T04:00:00.000Z	N/A
.extended.contact.values()	Indicator.Attribute	extended.contact.keys()	IBM DNS Admin	The Attribute Key is the value that it's on 'extended.contact.keys()'. Ex: Name
.extended.contactEmail	RelatedIndicator.Value	Email Address	dnsadm@us.ibm.com	N/A
.extended.registrarName	RelatedIndicator.Attribute	Registrar Name	CSC CORPORATE DOMAINS, INC.	N/A

Change Log

- **Version 1.1.1**
  - Correct/Enhance error handling
- **Version 1.1.0**
  - Restructuring the operation
- **Version 1.0.1**
  - Fix the issue with Malware Family
- **Version 1.0.0**
  - Initial release