ThreatQuotient

Whois XML API Operation User Guide

Version 1.0.0

November 03, 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	1.0.0
Compatible with ThreatQ Versions	>= 4.25.0
Support Tier	ThreatQ Supported

Introduction

The Whois XML API operation provides parsed information extracted from the raw Whois record and provides context in the form of attributes and indicators of compromise from the WhoisXmlApi operation.

The operation will extract additional information on FQDN indicator types using the Whois XML API endpoint.

Prerequisites

The following item is required for the operation:

- Whois Xml Api API Key

> ThreatQuotient does not issue third-party vendor credentials. Contact WhoisXMLAPI for the required key.

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	Enter the API Key fromWhois XML API.

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 Whois XML API operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Parse Information	Provides parsed information extracted from the raw Whois record.	Indicator	Indicator Attribute

Parse Information

Provides parsed information extracted from the raw Whois record. The URL that is called is:

```
https://whoisxmlapi.com/whoisserver/WhoisService?
outputformat=json&domainName={}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
createdDate	Created Date	Indicator Attribute	N/A	1997-09-15T00:00:00-0700	N/A
updatedDate	Update Date	Indicator Attribute	N/A	1997-09-15T00:00:00-0700	N/A
expiresDate	Expires Date	Indicator Attribute	N/A	1997-09-15T00:00:00-0700	N/A
registrant.organization	Registrant Organization	Indicator Attribute	N/A	Google LLC	N/A
registrant.state	Registrant State Indicator	Indicator Attribute	N/A	CA	N/A
registrant.country	Registrant Country Indicator	Indicator Attribute	N/A	United States	N/A
registrant.rawText	Registrant Raw Text Indicator	Indicator Attribute	N/A	Registrant Organization: Google LLC [...]	N/A
administrativeContact.organization	Administrative Contact Organization	Indicator Attribute	N/A	Google LLC	N/A
administrativeContact.country	Administrative Contact Country	Indicator Attribute	N/A	United States	N/A
administrativeContact.state	Administrative Contact State	Indicator Attribute	N/A	CA	N/A
administrativeContact.rawText	Administative Contact Raw Text	Indicator Attribute	N/A	Registrant Organization: Google LLC [...]	N/A
technicalContact.organization	Technical Contact Organization	Indicator Attribute	N/A	Google LLC	N/A
technicalContact.state	Technical Contact State	Indicator Attribute	N/A	CA	N/A
technicalContact.country	Technical Contact Country	Indicator Attribute	N/A	United States	N/A
technicalContact.rawText	Technical Contact Raw Text	Indicator Attribute	N/A	Registrant Organization: Google LLC [...]	N/A
nameServers.hostnames[]	FQDN	Related Indicator	N/A	ns2.google.com	N/A
nameServers.hostnames[]	FQDN	Related Indicator	N/A	11.11.11.11	N/A
status	Status	Indicator Attribute	N/A	ClientUpdatedProhibited	N/A
parseCode	Parse Code	Indicator Attribute	N/A	111	N/A
header	Header	Indicator Attribute	N/A	N/A	N/A
footer	Footer	Indicator Attribute	N/A	N/A	N/A
audit.createDate	Audit Created Date	Indicator Attribute	N/A	2018-10-23 15:33:41.000 UTC	N/A
audit.updatedDate	Audit Updated Date	Indicator Attribute	N/A	2018-10-23 15:33:41.000 UTC	N/A
customField1Name	Custom Field1 Name	Indicator Attribute	N/A	RegistrarContactEmail	N/A
customField2Name	Custom Field2 Name	Indicator Attribute	N/A	RegistrarContactEmail	N/A
customField3Name	Custom Field3 Name	Indicator Attribute	N/A	RegistrarContactEmail	N/A
customField1Value	Custom Field1 Value	Indicator Attribute	N/A	busecmplaints@markmonitor.com	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
customField2Value	Custom Field2 Value	Indicator Attribute	N/A	busecmplaints@markmonitor.com	N/A
customField3Value	Custom Field3 Value	Indicator Attribute	N/A	busecmplaints@markmonitor.com	N/A
registrarName	Registrar Name	Indicator Attribute	N/A	MarkMonitor	N/A
registrarIANAID	Registrar IANAID	Indicator Attribute	N/A	292	N/A
whoisServer	Whois Server	Indicator Attribute	N/A	whois.markmonitor.com	N/A
createdDateNormalized	Created Date Normalized	Indicator Attribute	N/A	1997-09-15 04:00:00 UTC	N/A
updatedDateNormalized	Updated Date Normalized	Indicator Attribute	N/A	1997-09-15 04:00:00 UTC	N/A
expiresDateNormalized	Expires Date Normalized	Indicator Attribute	N/A	1997-09-15 04:00:00 UTC	N/A
registryData.createdDate	Registry Created Date	Indicator Attribute	N/A	1997-09-15T04:00:00Z	N/A
registryData.expiresDate	Registry Expires Date	Indicator Attribute	N/A	1997-09-15T04:00:00Z	N/A
domainAvailability	Domain Availability	Indicator Attribute	N/A	Unavailable	N/A
contactEmail	Contact Email	Indicator Attribute	N/A	aaa@some.com	N/A
domainNameExt	Domain Name Ext	Indicator Attribute	N/A	.com	N/A
estimatedDomainAge	Estimated Domain Age	Indicator Attribute	N/A	1212	N/A
ips[]	IP Address	Related Indicator	N/A	12.12.12.12	N/A

Change Log

- **Version 1.0.0**
  - Initial release