ThreatQuotient

Digital Element NetAcuity Operation User Guide

Version 1.0.0

October 25, 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	>= 4.40.0
NetAcuity Server Version	6.4.2.1
Support Tier	ThreatQ Supported

Introduction

The Digital Element NetAcuity integration is an enrichment operation to geolocate and provide network information for IP Addresses from the NetAcuity database.

The operation provides the following action:

- **Geolocate IP Address** - performs a geolocation lookup for an IP Address.

The operation is compatible with IP Address type Indicators.

Prerequisites

User token from NetAcuity for the cloud offering, or an on-prem deployment for the NetAcuity Server version.

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
Hostname/IP Address of the NetAcuity Server	Enter the hostname or IP address of the NetAcuity instance. The default value is for the cloud offering. The Default is global.cloud.netacuity.com.
Communication Port	Optional - enter the port used for communication with NetAcuity. Otherwise, leave it blank.
User Token	Enter the user token for authentication.
Use HTTP	Check this box to use HTTP protocol when connecting to NetAcuity.
Verify SSL	Check this box to verify SSL when connecting to NetAcuity.

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
Geolocate IP Address	Lookup geolocation of IP addresses.	Indicators	IP Address

Geolocate IP Address

The Geolocate IP Address actions performs a geolocation of an IP address.

`GET https://<NetAcuity Host>/webservice/query`

Sample Response:


```
{
  "response": {
    "pulse-city-code": "2547",
    "pulse-postal-conf": "35",
    "pulse-region-full-name": "capital federal",
    "pulse-in-dst": "n",
    "pulse-city-conf": "90",
    "pulse-metro-name": "not metroized",
    "pulse-country": "arg",
    "pulse-city": "buenos aires",
    "pulse-postal-code": "c1431 cdy",
    "pulse-continent-code": "7",
    "pulse-gmt-offset": "-300",
    "vpn-proxy-names": "?",
    "pulse-timezone-name": "america/argentina/buenos_aires",
    "vpn-proxy-type": "hosting",
    "vpn-proxy-node": "?",
    "asn-name": "ripe network coordination centre",
    "pulse-metro-code": "-1",
    "vpn-proxy-description": "vpn",
    "pulse-continent-name": "south america",
    "pulse-localized-city-names": "buenos aires",
    "pulse-latitude": "-34.58",
    "isp-name": "panq b.v.",
    "pulse-region": "c",
    "ip": "91.206.168.63",
    "pulse-country-code": "32",
    "pulse-region-conf": "90",
    "pulse-two-letter-country": "ar",
```

```
    "pulse-country-full-name": "argentina",
    "pulse-country-conf": "99",
    "pulse-region-code": "12283",
    "pulse-conn-type": "wifi",
    "pulse-longitude": "-58.49",
    "pulse-conn-speed": "broadband",
    "pulse-area-codes": "?",
    "asn": "209854"
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.pulse-conn-type	Attribute	attribute.name.Connection Type	NA	wifi
response.pulse-conn-speed	Attribute	attribute.name.Connection Speed	NA	broadband
response.pulse-latitude	Attribute	attribute.name.Latitude	NA	-34.58
response.pulse-longitude	Attribute	attribute.name.Longitude	NA	-58.49
response.pulse-continent-code	Attribute	attribute.name.Continent Code	NA	7
response.pulse-continent-name	Attribute	attribute.name.Continent	NA	south america
response.pulse-two-letter-country	Attribute	attribute.name.Country Code	NA	ar
response.pulse-country-code	Attribute	attribute.name.Country Num Code	NA	32
response.pulse-country-full-name	Attribute	attribute.name.Country	NA	argentina
response.pulse-region	Attribute	attribute.name.Region	NA	c
response.pulse-region-code	Attribute	attribute.name.Region Code	NA	12283
response.pulse-region-full-name	Attribute	attribute.name.Region Name	NA	capital federal
response.pulse-metro-name	Attribute	attribute.name.Metropolitan Area	NA	not metroized
response.pulse-metro-code	Attribute	attribute.name.Metropolitan Area Code	NA	-1
response.pulse-localized-city-names	Attribute	attribute.name.Localized City Name	NA	buenos aires
response.pulse-city	Attribute	attribute.name.City	NA	buenos aires
response.pulse-city-code	Attribute	attribute.name.City Code	NA	2547
response.pulse-postal-code	Attribute	attribute.name.Postal Code	NA	c1431 cdy
response.pulse-area-codes	Attribute	attribute.name.Area Code	NA	
response.pulse-timezone-name	Attribute	attribute.name.Time Zone	NA	america/argentina/ buenos_aires
response.isp-name	Attribute	attribute.name.ISP	NA	panq b.v.
response.asn-name	Attribute	attribute.name.ASN Name	NA	ripe network coordination centre
response.asn	Attribute	attribute.name.ASN	NA	209854
response.vpn-proxy-names	Attribute	attribute.name.VPN Proxy Names	NA	
response.vpn-proxy-type	Attribute	attribute.name.VPN Proxy Type	NA	hosting
response.vpn-proxy-node	Attribute	attribute.name.VPN Proxy Node	NA	
response.vpn-proxy-description	Attribute	attribute.name.VPN Proxy Description	NA	vpn

Change Log

- **Version 1.0.0**
  - Initial release