ThreatQuotient

IBM QRadar Action

Version 1.0.0

July 28, 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	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The IBM QRadar Action for ThreatQ allows an analyst to query IBM QRadar for more information about a given IOC.

The integration provides the following action:

- **IBM QRadar Action -** performs a lookup within QRadar to find logs related to an indicator.

The action is compatible with the following indicator types:

- Email Address
- FQDN
- IP Address
- URL

The action returns enriched system indicator and event object types.

> 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 QRadar Host and SEC Token
- A data collection containing at least one of the following indicator types:
  - Email Address
  - FQDN
  - IP Address
  - 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 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.

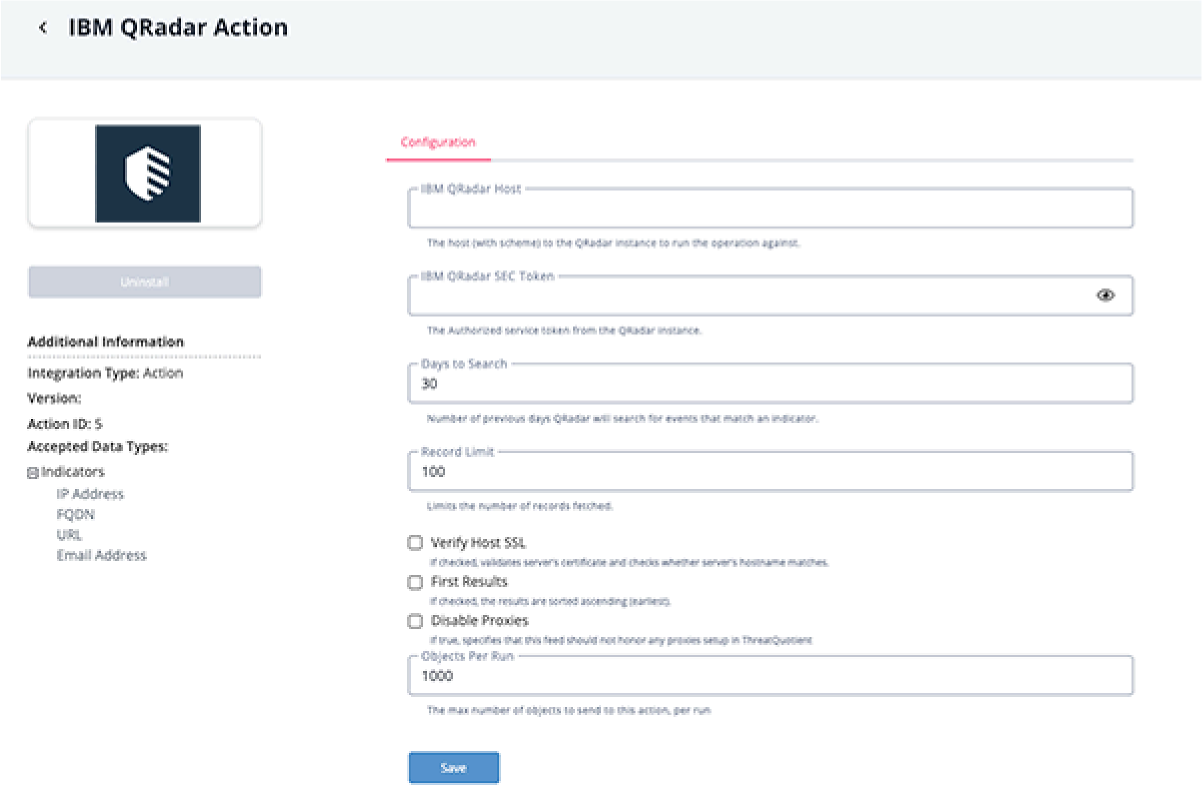
To configure the integration:

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.

PARAMETER	DESCRIPTION
IBM QRadar Host	The host (with scheme) to the QRadar instance to run the operation against.
IBM QRadar SEC Token	The Authorized service token from the QRadar instance.
Days to Search	Number of previous days QRadar will search for events that match an indicator.
Record Limit	Limits the number of records fetched.
Verify Host SSL	If enabled, validates server's certificate and checks whether server's hostname matches.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
First Results	If enabled, the results are sorted ascending (earliest).

PARAMETER	DESCRIPTION
Objects Per Run	The max number of objects to send to this action, per run.



Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

⊟ Indicators
- IP Address
- FQDN
- URL
- Email Address

IBM QRadar Host:

The host (with scheme) to the QRadar instance to run the operation against.

IBM QRadar SEC Token:

The Authorized service token from the QRadar instance.

Days to Search: 30

Number of previous days QRadar will search for events that match an indicator.

Record Limit: 100

Limits the number of records fetched.

☐ Verify Host SSL

If checked, validates server's certificate and checks whether server's hostname matches.

☐ First Results

If checked, the results are sorted ascending (earliest).

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Objects Per Run: 1000

The max number of objects to send to this action, per run

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 QRadar Action	Send Query to IBM QRadar for the IOC and get back the results	Indicators	Email Address, IP Address, FQDN, URL

IBM QRadar Action

The IBM QRadar Action send a query to IBM QRadar for a given IOC and retrieves the results.

```
POST https://'{{qradar_host}}/api/ariel/searches?query_expression=SELECT
LOGSOURCENAME(logsourceid), * FROM events + WHERE UTF8(payload) ILIKE
'{{object.value}}' AND CATEGORYNAME(category) != 'SIM User Action' +ORDER BY
starttime {{'ASC' if first_result else 'DESC'}} LIMIT {{record_limit}} LAST
{{days_to_search}} DAYS
```

Sample Response:

```
{
    "cursor_id": "a4a5781f-b88d-4108-91c3-4d724d9675be",
    "status": "WAIT",
    "compressed_data_file_count": 0,
    "compressed_data_total_size": 0,
    "data_file_count": 0,
    "data_total_size": 0,
    "index_file_count": 0,
    "index_total_size": 0,
    "processed_record_count": 0,
    "desired_retention_time_msec": 86400000,
    "progress": 0,
    "progress_details": [],
    "query_execution_time": 0,
    "query_string": "SELECT LOGSOURCENAME(logsourceid), * FROM events   WHERE
sourceip = '10.114.3.34' OR destinationip = '10.114.3.34'  ORDER BY starttime
DESC LIMIT 0 LAST 1 DAYS",
    "record_count": 0,
    "size_on_disk": 0,
    "save_results": false,
    "completed": false,
    "subsearch_ids": [],
    "snapshot": null,
    "search_id": "a4a5781f-b88d-4108-91c3-4d724d9675be"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.search_id	Indicator.Attribute	IBM QRadar Search ID	N/A	`a4a5781f-b88d-4108-91c3-4d724d9675be`	N/A
.status	Indicator.Attribute	IBM QRadar Search Status	N/A	`WAIT`	If the value is different than 'COMPLETED' it updates the value

Retrieve Sighting Information (Supplemental)

`GET https://{{qradar_host}}/api/ariel/searches/{{search_id}}/results`

Sample Response

```
{
  "events": [
    {
      "logsourcename_logsourceid": "Health Metrics-2 :: qradar75",
      "starttime": 1720263000505,
      "protocolid": 255,
      "sourceip": "10.114.3.34",
      "logsourceid": 69,
      "qid": 94000001,
      "sourceport": 0,
      "eventcount": 1,
      "magnitude": 5,
      "identityip": "0.0.0.0",
      "destinationip": "127.0.0.1",
      "destinationport": 0,
      "category": 8052,
      "username": null
    },
    {
      "logsourcename_logsourceid": "Health Metrics-2 :: qradar75",
      "starttime": 1720263000505,
      "protocolid": 255,
      "sourceip": "10.114.3.34",
      "logsourceid": 69,
      "qid": 94000001,
      "sourceport": 0,
      "eventcount": 1,
      "magnitude": 5,
      "identityip": "0.0.0.0",
      "destinationip": "127.0.0.1",
      "destinationport": 0,
      "category": 8052,
      "username": null
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this supplemental action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
events[0].starttime	Event.Attribute	First Sighting	N/A	`2024-07-07 07:26:39+00:00`	We use a timestamp filter to convert the epoch time to date
events[len(events)-1].starttime	Event.Attribute	Last Sighting	N/A	`2024-07-08 06:50:33+00:00`	We use a timestamp filter to convert the epoch time to date
len(events)	Event.Attribute	Total Sightings	N/A	`36`	The value gets updated if new data is found
N/A	Event.Attribute	IBM QRadar Search Query	N/A	`SELECT LOGSOURCENAME(logsourceid), * FROM events WHERE UTF8(payload) ILIKE '{{object.value}}' AND CATEGORYNAME(category) != 'SIM User Action' ORDER BY starttime {{'ASC' if first_result else 'DESC'}} LIMIT {{record_limit}} LAST {{days_to_search}} DAYS`	N/A

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.

METRIC	RESULT
Run Time	1 minute
Indicators	6
Events	6
Event Attributes	18

Use Case Example

1. A Threat Analyst identifies a collection of supported objects he/she would like to enrich.
2. The Threat Analyst adds the IBM QRadar Action to a Workflow.
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
4. The Workflow executes all Actions in the graph, including IBM QRadar.
5. The Workflow enriches the objects with IBM QRadar data.

Known Issues / Limitations

- This action has three different scenarios depending on the attributes of the object:
  1. The action runs and searches for `IBM QRadar Search ID` and `IBM QRadar Search Status` attributes. If not present, create a new search and add those attributes to the Indicator.
  2. The `IBM QRadar Search ID` and `IBM QRadar Search Status` attributes are present but `IBM QRadar Search Status` is different from COMPLETE. Recheck the status of the search.
  3. The `IBM QRadar Search ID` and `IBM QRadar Search Status` attributes are present and `IBM QRadar Search Status` is COMPLETE. The search is complete and fetches the results. If there's a result, an event will be created. The `IBM QRadar Search ID` and `IBM QRadar Search Status` attributes are deleted.
- Please ensure that, prior to rerunning the action, sufficient time is allowed for the database to update all values.

Change Log

- **Version 1.0.0**
    - Initial release