

ThreatQuotient



ServiceNow Action Guide

Version 1.0.0

May 23, 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

| | |
|--|----|
| Integration Details | 5 |
| Introduction | 6 |
| Prerequisites | 7 |
| Installation | 8 |
| Configuration | 9 |
| Actions | 12 |
| ServiceNow - Create Ticket | 12 |
| ServiceNow Ticket Type Table Mapping | 14 |
| Get Observable (Supplemental) | 15 |
| Create Observable (Supplemental) | 15 |
| Create Relationship (supplemental) | 16 |
| Enriched Data | 17 |
| Use Case Example | 18 |
| Known Issues / Limitations | 19 |
| Change Log | 20 |

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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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 | >= 5.14.0 |
| ThreatQ TQO License Required | Yes |
| Support Tier | ThreatQ Supported |

Introduction

The ServiceNow action for ThreatQuotient enables a user to create tickets and observables in ServiceNow.

The integration provides the following action:

- **ServiceNow - Create Ticket** - creates tickets and observables in ServiceNow based on TQ indicators. For each indicator, an observable will be created in ServiceNow that will be linked to the newly created ticket. The ThreatQ objects will be updated with attributes mapped to the items in ServiceNow.

The action is compatible with the following system object types:

- IP Address
- IPv6 Address
- MD5
- SHA-1
- SHA-256
- SHA-512

The action returns enriched indicators and indicator attributes system objects.



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 objects:
 - IP Address
 - IPv6 Address
 - MD5
 - SHA-1
 - SHA-256
 - SHA-512

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 |
|--------------------------|---|
| Hostname | Your ServiceNow Hostname. |
| Username | Your ServiceNow Username. |
| Password | Your ServiceNow Password. |
| Ticket Creation Behavior | Select the creation behavior. Options include: <ul style="list-style-type: none">◦ A Single ticket / case with all items linked (default)◦ Individual tickets / cases per item |
| Ticket / Case Type | Select the type of ticket / case to create in ServiceNow. Options include: <ul style="list-style-type: none">◦ Security Incident (default) |

| PARAMETER | DESCRIPTION |
|--|---|
| | <ul style="list-style-type: none">◦ Incident◦ Security Incident Response Task◦ Security Case |
| Name | This populates the ticket / case name in ServiceNow. |
| Description | This is an optional field where users can provide a description for the case / ticket created. |
| Observable Rating | Select the rating for each observable attached to the ticket / case in ServiceNow. Options include: <ul style="list-style-type: none">◦ Malicious (default)◦ Unknown |
| Append ticket / case name with object name | <p>By checking this box it will append the indicator value to the "Name" provided.</p> <div> This parameter is only available if you have select Individual Tickets / Cases per item option for the Ticket / Case Type parameter.</div> |
| Requests per minute | <p>The maximum number of requests to make to ServiceNow per-minute. The default value is 100.</p> <div> This parameter is only available if you have select Individual Tickets / Cases per item option for the Ticket / Case Type parameter.</div> |
| Objects per run | The maximum number of objects to send to ServiceNow per-run. The default value is 5000. |

PARAMETER

DESCRIPTION



This parameter is only available if you have select **Individual Tickets / Cases per item** option for the **Ticket / Case Type** parameter.



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Configuration

Hostname

ServiceNow Hostname

Username

ServiceNow Username used to authenticate

Password



Ticket Creation Behavior

A single ticket / case with all items linked



Select the creation behavior

Ticket / Case Type

Security Incident



Select the type of ticket / case to create in ServiceNow

Name

This populates the ticket / case name in ServiceNow

Description (optional)

This is an optional field where users can provide a description for the case / ticket created

Observable Rating

Malicious



Select the rating for each observable attached to the ticket / case in ServiceNow

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

| ACTION | DESCRIPTION | OBJECT TYPE | OBJECT SUBTYPE |
|--|--|-------------|---|
| ServiceNow - Create Ticket | Creates tickets and observables in ServiceNow based on TQ indicators. Enrich the ThreatQ objects with attributes mapped to the items in ServiceNow | Indicators | IP Address, IPv6 Address, URL, FQDN, MD5, SHA-1, SHA-256, SHA-512 |

ServiceNow - Create Ticket

The ServiceNow - Create Ticket action creates tickets in ServiceNow based on ThreatQ indicators. For each indicator, an observable will be created in ServiceNow that will be linked to the newly created ticket. The ThreatQ objects will be updated with attributes mapped to the items in ServiceNow.

```
POST {{host}}/api/now/table/{{table_name}}?sysparm_fields=sys_id,number
```

Sample Request:

```
{
  "short_description": "Block address - 8.8.8.8",
  "description": "This is a test description"
}
```

Sample Response:

```
{
  "result": {
    "sys_id": "bd50ee481b181d1014a264207e4bcb8a",
    "number": "INC0010058"
  }
}
```

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|----------------|---------------------------------------|--------------------------------------|----------------|--|--|
| result.sys_id | Event.Attribute / Indicator.Attribute | ServiceNow Ticket URL | N/A | https://ven04019.service-now.com/nav_to.do?uri=%2Fsn_incident.do%3Fsys_id%3D50ee481b181d1014a264207e4bcb8a | Formatted as {{host}}/nav_to.do?uri=%2F{{{table_name}}}.do%3Fsys_id%3D{{{sys_id}}} |
| result.number | Event.Attribute / Indicator.Attribute | ServiceNow Ticket Number | N/A | INC0010058 | N/A |

ServiceNow Ticket Type Table Mapping

The following is a mapping table for ServiceNow ticket types and naming conventions.

| TICKET TYPE | SERVICENOW TABLE NAME |
|-------------------|-----------------------|
| Incident | incident |
| security_incident | sn_si_incident |
| security_task | sn_si_task |
| security_case | sn_ti_case |

Get Observable (Supplemental)

Retrieves the observable sys_id from ServiceNow for indicator_value if exists

```
GET {{host}}/api/now/table/sn_ti_observable?sysparm_query=value={{indicator_value}}
&sysparm_fields=sys_id
```

Sample Response:

```
{
  "result": {
    "sys_id": "bd50ee481b181d1014a264207e4bcb8a"
  }
}
```

Create Observable (Supplemental)

Creates an observable and retrieves the sys_id from ServiceNow for indicator_value if it does not exist

```
POST {{host}}/api/now/table/sn_ti_observable?sysparm_fields=sys_id
```

Sample Request:

```
{
  "value": "1.0.1.0",
  "type": "IP address (V4)",
  "finding": "Malicious"
}
```

Sample Response:

```
{
  "result": {
    "sys_id": "bd50ee481b181d1014a264207e4bcb8a"
  }
}
```

ThreatQ provides the following default mapping for Get and Create Observable:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|----------------|---------------------------------------|--------------------------------------|----------------|---|--|
| result.sys_id | Event.Attribute / Indicator.Attribute | ServiceNow Observable URL | N/A | https://ven04019.service-now.com/nav_to.do?uri=%2Fsn_ti_observable.do%3Fsys_id%3Dbd50ee481b181d1014a264207e4bcb8a | Formatted as {{host}}/nav_to.do?uri=%2Fsn_ti_observable.do%3Fsys_id%3Dbd50ee481b181d1014a264207e4bcb8a |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|-------------------|----------------|---|-------------------|----------|---------------------------|
| | | | | | do%3Fsys_id%3D{{sys__id}} |

Create Relationship (supplemental)

Creates a relationship between ticket and observable in ServiceNow

POST {{host}}/api/now/table/sn_ti_m2m_task_observable?sysparm_fields=sys_id

Sample Request:

```
{
  "task": "bd50ee481b181d1014a264207e4bcb8a",
  "observable": "bd50ee481b181d1014a264207e4bcb8a"
}
```

Sample Response:

```
{
  "result": {
    "sys_id": "30ffdb5e1ba1e91014a264207e4bcb80"
  }
}
```


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 | 2 |
| Indicators Attributes | 6 |

Use Case Example

1. A user submits a data collection using the `ServiceNow - create ticket` action to the ServiceNow with a data collection containing 100 system objects (100 IP Address).
2. The ServiceNow creates tickets and observables for submitted data and establishes a relationship between them.
3. The action returns the submitted data collection enriched the following:
 - 100 Indicators
 - 300 indicator attributes

Known Issues / Limitations

- The ThreatQ platform limits the incoming list of values to 100. If the collection is bigger than that, even if the user selects to create a single ticket that links all the items, multiple tickets will be created per 100. Example: incoming list of 450 will result in the creation of 5 tickets.

Change Log

- Version 1.0.0
 - Initial release