ThreatQuotient

ServiceNow Action User Guide

Version 1.1.0

January 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	1.1.0
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. For each indicator, an observable will be created in ServiceNow that will be linked to the newly created ticket. ThreatQ objects that are not mapped as indicators will be created in ServiceNow and associated attributes mapped to items in ServiceNow.

See the ServiceNow to ThreatQ Object Mapping table for more details.

The integration provides the following action:

- **ServiceNow - Create Ticket** - creates tickets and observables in ServiceNow based on ThreatQ indicators and objects.

The action is compatible with the following system object types:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Course of Actions
- Exploits
- Targets
- Identities
- Indicators
- Intrusion Sets
- Malware
- Reports
- Tools
- TTPs
- Vulnerabilities

The action returns the following enriched object types:

- Adversaries
  - Adversary Attributes
- Assets
  - Asset Attributes
- Attack Patterns
  - Attack Pattern Attributes
- Campaigns
  - Campaign Attributes
- Course of Actions
  - Course of Action Attributes
- Exploit Targets
  - Exploit Target Attributes
- Identities
  - Identity Attributes
- Indicators
  - Indicator Attributes
- Intrusion Sets
  - Intrusion Set Attributes
- Malware
  - Malware Attributes
- Reports
  - Report Attributes
- Tools
  - Tool Attributes
- TTPs
  - TTP Attributes
- Vulnerabilities
  - Vulnerability Attributes

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 ServiceNow Username and Password.
- A data collection containing at least one of the following object types:
  - Adversary
  - Asset
  - Attack Pattern
  - Campaign
  - Course of Action
  - Exploit
  - Target
  - Identity
  - Indicator
  - Intrusion Set
  - Malware
  - Report
  - Tool
  - TTP
  - Vulnerability

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.

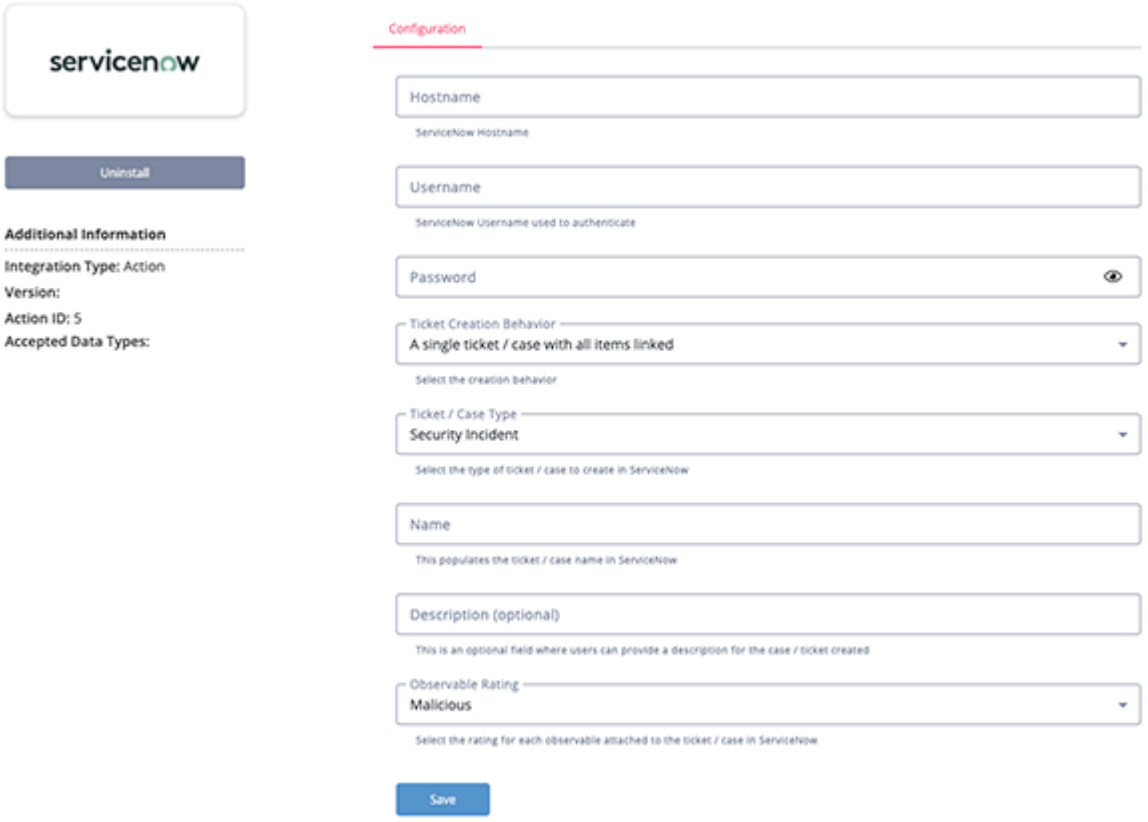
To configure the integration:

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: ◦ 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: ◦ Security Incident (default) ◦ Incident ◦ Security Incident Response Task ◦ Security Case
Name	This populates the ticket / case name in ServiceNow.

PARAMETER	DESCRIPTION
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: ◦ Malicious (default) ◦ Unknown
Append ticket / case name with object name	By checking this box it will append the indicator value to the "Name" provided.  This parameter is only available if you have select **Individual Tickets / Cases per item** option for the **Ticket / Case Type** parameter.
Requests per minute	The maximum number of requests to make to ServiceNow per-minute. The default value is 100.  This parameter is only available if you have select **Individual Tickets / Cases per item** option for the **Ticket / Case Type** parameter.
Objects per run	The maximum number of objects to send to ServiceNow per-run. The default value is 5000.  This parameter is only available if you have select **Individual Tickets / Cases per item** option for the **Ticket / Case Type** parameter.



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 ThreatQ objects.	Adversary, Asset, Attack Pattern, Campaign, Course of Action, Exploit Target, Identity, Indicator, Intrusion Set, Malware, Report, Tool, TTP, Vulnerability	Indicators - All Types

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_si_incident.do%3Fsys_id%bd50ee481b181d1014a264207e4bcb8a	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)

The Get Observable supplemental action retrieves the observable sys_id from ServiceNow for indicator_value if exists.

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

The `object_type` is determined using the ServiceNow to ThreatQ Object Type Mapping table.

Sample Response:

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

Create Observable (Supplemental)

The Create Observable supplemental action creates an observable and retrieves the sys_id from ServiceNow for indicator_value id 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	Adversary / Asset / Attack Pattern / Campaign / Course of Action / Exploit Target / Identity / Indicator / Intrusion Set / Malware / Report / Tool / TTP / Vulnerability.Attribute	ServiceNow Observable URL	N/A	https://ven04019.service-now.com/nav_to.do?uri=%2Fsn_ti_observable.do%3Fsys_id%bd50ee481b181d1014a264207e4bcb8a	Formatted as `{{host}}/nav_to.do?uri=%2Fsn_ti_observable.do%3Fsys_id%3D{{sys__id}}`

ServiceNow Indicator Type to ThreatQ Type Mapping

The following is a mapping table for Service Now Types to ThreatQ indicator types.

TICKET TYPE	SERVICENOW TABLE NAME
Autonomous System Number	ASN
CVE number	CVE
IP address (V4)	IP Address
IP address (V6)	IPv6 Address
CIDR rule	CIDR Block
MAC address	MAC Address
MUTEX name	Mutex
MD5 hash	MD5
SHA1 hash	SHA-1
SHA256 hash	SHA-256
SHA512 hash	SHA-512
SHA384 hash	SHA-384
Domain name	FQDN
URL	URL
Email address	Email Address

TICKET TYPE	SERVICENOW TABLE NAME
Email subject	Email Subject
File Name	Filename
File Path	File Path
Registry key	Registry Key
Username	Username

Create Relationship (supplemental)

The Create Relationship supplemental action 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"
    }
}
```

Create Object Supplemental

The Create Object supplemental action creates an object and retrieves the sys_id from ServiceNow if the object does not exist.

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

Sample Request:

```
{
    "name": "APT34",
    "description": "Object imported from ThreatQ Adversary when ticket
SIR0010047 was created.",
    "created": "2024-01-17T04:56:19.000Z",
    "modified": "2024-01-17T04:56:19.000Z"
}
```

Sample Response:

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

ThreatQ provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result.sys_id	Adversary / Asset / Attack Pattern / Campaign / Course of Action / Exploit Target / Identity / Indicator / Intrusion Set / Malware / Report / Tool / TTP / Vulnerability.Attribute	ServiceNow Object URL	N/A	https://ven04019.service-now.com/nav_to.do?uri=%2Fsn_ti_stix2_threat_actor.do%3Fsys_id%bd50ee481b181d1014a264207e4bcb8a	Formatted as `{{host}}/nav_to.do?uri=%2F{{object_type}}.do%3Fsys_id%3D{{sys_id}}`

ServiceNow to ThreatQ Object Mapping

The following table illustrates ServiceNow to ThreatQ object mapping.

SERVICENOW OBJECT	THREATQ OBJECT
sn_ti_stix2_threat_actor	Adversary
sn_ti_observable	Asset
sn_ti_stix2_attack_pattern	Attack Pattern
sn_ti_stix2_campaign	Campaign
sn_ti_stix2_course_of_action	Course of Action
sn_ti_observable	Exploit Target
sn_ti_stix2_identity	Identity
sn_ti_observable	Indicator
sn_ti_stix2_intrusion_set	Intrusion Set
sn_ti_stix2_malware	Malware
sn_ti_stix2_threat_report	Report
sn_ti_stix2_tool	Tool
sn_ti_attack_mode	TTP
sn_ti_stix2_vulnerability	Vulnerability

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	24 minutes
Indicators	100
Indicator Attributes	300
Adversaries	100
Adversary Attributes	300
Asset	100
Asset Attributes	300
Attack Patterns	100
Attack Pattern Attributes	300
Campaigns	100
Campaign Attributes	300
Course of Action	100
Course of Action Attributes	300

METRIC	RESULT
Exploit Targets	100
Exploit Target Attributes	300
Identities	100
Identity Attributes	300
Intrusion Sets	100
Intrusion Set Attributes	300
Malware	100
Malware Attributes	300
Reports	100
Report Attributes	300
Tools	100
Tool Attributes	300
TTP	100
TTP Attributes	300
Vulnerabilities	100
Vulnerability Attributes	300

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 1.1.0**
  - Added compatibility support for all ThreatQ indicator types.
  - Added compatibility support for the following object types:
    - Adversary
    - Asset
    - Attack Pattern
    - Campaign
    - Course of Action
    - Exploit Target
    - Identity
    - Intrusion Set
    - Malware
    - Report
    - Tool
    - TTP
    - Vulnerability
- **Version 1.0.0**
  - Initial release