

ThreatQuotient



ServiceNow Operation User Guide

Version 1.1.1 rev-a

July 17, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

- Warning and Disclaimer 3
- Support 4
- Integration Details..... 5
- Introduction 6
- Prerequisites 7
 - ServiceNow Plugins Installation 7
- Installation..... 8
- Configuration 9
- Actions 10
 - Create Security Incident..... 11
 - Action Parameters..... 15
 - Add Observable..... 17
 - Action Parameters..... 18
 - Add Ticket..... 19
 - Action Parameters..... 21
- Change Log 23

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	1.1.1
Compatible with ThreatQ Versions	>= 4.40.0
Compatible with ServiceNow Versions	Utah, Tokyo, San Diego
Support Tier	ThreatQ Supported

Introduction

The ServiceNow Operation for ThreatQuotient enables a user to perform actions, such as enrichment, against the ServiceNow API.

The operation provides the following actions:

- **Create Security Incident** - creates a Security Incident in SNOW from a TQ Indicator. It will also add the observable to ServiceNow and relate the incident to it.
- **Add Observable** - adds (or updates) an observable in ServiceNow based off a TQ indicator.
- **Add Ticket** - creates (or updates) a ticket in ServiceNow from any TQ event; includes the related indicators as observables.

The operation is compatible with indicators and events.

Prerequisites

The integration requires the installation of three plugins on your ServiceNow instance.

ServiceNow Plugins Installation

There are three plugins which must be installed in the following order:

1. Threat Intelligence
2. Vulnerability Response
3. Security Incident Response

To install these plugins, log into your ServiceNow instance and complete the following steps:

1. From the filter navigation, search for plugins.
2. Click **Plugins**.
3. Locate each plugin, select it, and navigate to the plugin page.
4. Click the plugin name.
5. Under related links, select **Activate/Update**.



A progress bar indicates the progress of the activation. The modal updates when the activation is complete.

6. To continue installing plugins, click **View Plugin List** and repeat the steps above.
7. After you install the final plugin, select **Close Reload Form**.

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
Host	Your ServiceNow hostname.
Password	Your ServiceNow password.
TQ Host	Your ThreatQ hostname.
Username	Your ServiceNow Username

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 uses pysnow Client and Resource to communicate with ServiceNow.

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Create Security Incident	Create Security Incident in SNOW from a TQ Indicator. It will also add the observable to ServiceNow and relate the incident to it. Lastly, it will upload the corresponding ServiceNow incident, as an Event, to ThreatQ.	Indicators	MD5, SHA-1, SHA-256, SHA-512, IP Address, FQDN, URL, Email Address, Registry Key, CIDR Block, Mutex, CVE, ASN, MAC Address, Email Subject, String
Add Observable	Add (or update) an observable in ServiceNow based off a TQ indicator	Indicators	MD5, SHA-1, SHA-256, SHA-512, IP Address, FQDN, URL, Email Address, Registry Key, CIDR Block, Mutex, CVE, ASN, MAC Address, Email Subject, String
Add Ticket	Creates (or updates) a ticket in ServiceNow from any TQ event; includes the related indicators as observables	Events	Any

Create Security Incident

This action will create a new security incident in ServiceNow. It will also add the observable to ServiceNow and relate the incident to it. Lastly, it will upload the corresponding ServiceNow incident, as an Event, to ThreatQ.

PUT https://<SNOW Host>/api/now/table/sn_si_incident to create the SNOW ticket

Sample Response:

```
{
  "sys_updated_by": "admin",
  "new_pir_respondents": "",
  "upon_reject": "Cancel all future Tasks",
  "special_access_read": "",
  "secure_notes": "",
  "time_worked": "",
  "pir_respondents": "",
  "department": "",
  "problem": "",
  "phish_email": "",
  "sla_suspended": "false",
  "description": "",
  "request_category": "",
  "contract": "",
  "sys_updated_on": "2021-05-04 11:47:47",
  "correlation_id": "",
  "sla_suspended_for": "",
  "affected_user": "",
  "vulnerability": "",
  "spam": "false",
  "source_ip": "",
  "sys_created_by": "admin",
  "closed_by": "",
  "comments_and_work_notes": "2021-05-04 11:47:47 - System Administrator
(Automation activity)\nRisk score changed from Empty to 40 due to change in
business impact, priority, severity, risk score override\n\n",
  "user_input": "",
  "automation_activity": "2021-05-04 11:47:47 - System Administrator
(Automation activity)\nRisk score changed from Empty to 40 due to change in
business impact, priority, severity, risk score override\n\n",
  "short_description": "Observable Sighting: 81.69.35.30",
  "malware_hash": "",
  "sla_due": "UNKNOWN",
  "active": "true",
  "approval_set": "",
  "activity_due": "UNKNOWN",
  "assignment_group": {
    "link": "https://ven04019.service-now.com/api/now/table/
sys_user_group/dea26263ff0331007a6dffffffffffff19",
```

```

        "display_value": "Security Incident Assignment"
    },
    "parent_security_incident": "",
    "category": null,
    "work_end": "",
    "alert_sensor": "",
    "initiated_from": "",
    "vendor_reference": "",
    "sys_created_on": "2021-05-04 11:47:47",
    "opened_at": "2021-05-04 11:47:47",
    "delivery_task": "",
    "urgency": "3 - Low",
    "risk_score": "40",
    "dest_ip": "",
    "delivery_plan": "",
    "due_date": "",
    "sys_domain_path": "/",
    "approval": "Not Yet Requested",
    "is_catalog": "false",
    "business_criticality": "3 - Non-critical",
    "pir": null,
    "cmdb_ci": "",
    "subcategory": null,
    "comments": "",
    "state": "Draft",
    "previous_agent": "",
    "caller": "",
    "expected_start": "",
    "sys_id": "94657d6b1bf7ec50cf41cbb5624bcb37",
    "other_ioc": "",
    "escalation": "Normal",
    "business_duration": "",
    "security_incident_self": {
        "link": "https://ven04019.service-now.com/api/now/table/
sn_si_incident/94657d6b1bf7ec50cf41cbb5624bcb37",
        "display_value": "SIR0010052"
    },
    "additional_assignee_list": "",
    "assigned_vendor": "",
    "close_notes": "",
    "priority": "4 - Low",
    "sys_domain": {
        "link": "https://ven04019.service-now.com/api/now/table/
sys_user_group/global",
        "display_value": "global"
    },
    "qualification_group": "",
    "risk_change": "Up",
    "prediction": null,
    "work_start": "",

```

```

    "knowledge": "false",
    "sys_mod_count": "0",
    "sys_class_name": "Security Incident",
    "request_type": null,
    "correlation_display": "",
    "opened_for": {
      "link": "https://ven04019.service-now.com/api/now/table/sys_user/6816f79cc0a8016401c5a33be04be441",
      "display_value": "System Administrator"
    },
    "location": "",
    "service_offering": "",
    "opened_by": {
      "link": "https://ven04019.service-now.com/api/now/table/sys_user/6816f79cc0a8016401c5a33be04be441",
      "display_value": "System Administrator"
    },
    "reassignment_count": "0",
    "template_workflow_invoked": "false",
    "malware_url": "",
    "work_notes": "",
    "sys_tags": "",
    "attack_vector": "",
    "contact_type": null,
    "number": "SIR0010052",
    "upon_approval": "Proceed to Next Task",
    "severity": "2 - Medium",
    "asset": "",
    "substate": "",
    "special_access_write": "",
    "order": "",
    "risk": "Moderate",
    "task_created": "false",
    "impact": "3 - Low",
    "external_url": "",
    "made_sla": "true",
    "assigned_to": "",
    "estimated_end": "",
    "follow_up": "",
    "change_request": "",
    "watch_list": "",
    "calendar_duration": "",
    "sla_suspended_on": "",
    "sla_suspended_reason": null,
    "parent": "",
    "company": "",
    "risk_score_override": "false",
    "referrer_url": "",
    "expected_end": "",
    "template": "",

```

```

    "skills": "",
    "billable": "false",
    "approval_history": "",
    "universal_request": "",
    "route_reason": "",
    "close_code": null,
    "business_service": "",
    "incident": "",
    "requested_due_by": "",
    "task_effective_number": "SIR0010052",
    "security_tags": "",
    "work_notes_list": "",
    "group_list": "",
    "confidence_score": "",
    "closed_at": ""
  }

```




This action also uses `.../table/sn_ti_observable`, `.../sn_ti_m2m_task_observable`, and `.../table/sn_sec_cm_n_security_annotation` to create the observable, relate the observable, and add security annotations to the observable.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH (TABLE.KEY)	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY
sn_si_incident.work_notes	Event	event.comments
sn_si_incident.description	Event	event.description
sn_ti_observable.value	Indicator	indicator.value
sn_ti_observable.type.display_value	Indicator	indicator.type.name
sn_sec_cm_n_security_annotation.annotation	Indicator	indicator.score
sn_sec_cm_n_security_annotation.annotation	Indicator	indicator.status

Action Parameters

The Create Security Incident action offers the following configuration parameters:

PARAMETER	DESCRIPTION
Short Description	<p>Optional - Enter a title value for this incident. if left blank, Observable Sighting: {indicator} will be used.</p> <div>  <p>You can format the indicator value into your custom description by putting {} where you want the indicator value to go.</p> </div>
Description	Optional - Enter a long description for the security incident.
Category	Select a category (or None) to give to this security incident.
Setting Risk Score	<p>Select how you want to set the Risk Score of the security incident.</p> <p>Options include:</p> <ul style="list-style-type: none"> • Map ThreatQ Score to Risk Score (default) • Set to Custom Risk Score Below • Do Not Set Risk Score
Custom Risk Score	Enter a custom risk score to use when Set to Custom Risk Score Below is selected.
Observable Finding	<p>Select the "finding" for the observable.</p> <p>Options include:</p> <ul style="list-style-type: none"> • Malicious (default) • Unknown

Operation: ServiceNow

×

Short Description (Optional)

Observable Sighted in ESM: {}

Enter a title value for this incident. If left blank, "Observable Sighting: {{Indicator}}" will be used. You can format the indicator value into your custom description by putting {{}} where the you want the indicator value to go.

Description (Optional)

Triage this malicious indicator

G

Enter a description for the incident

Category

Malware

▼

Select a category for this incident

Setting Risk Score

Set to Custom Risk Score Below

▼

Select how you would like the risk score to be set

Custom Risk Score

100

Enter a custom risk score to use when "Set to Custom Risk Score Below" is selected

Observable Finding

Malicious

▼

Select what "finding" you want to give the observable

Run

Cancel

Add Observable

This action adds (or updates) an observable in ServiceNow.

PUT https://<SNOW Host>/api/now/table/sn_ti_observable

Sample Response:

```
{
  "sys_tags": "",
  "finding": "Malicious",
  "sys_domain": {
    "display_value": "global",
    "link": "https://ven04019.service-now.com/api/now/table/
sys_user_group/global"
  },
  "sys_updated_by": "admin",
  "notes": "",
  "sighting_count": "1",
  "sys_id": "c665352f1bf7ec50cf41cbb5624bcb90",
  "type": {
    "display_value": "IP address (V4)",
    "link": "https://ven04019.service-now.com/api/now/table/
sn_ti_observable_type/5d0b43809f81120035c6786f957fcf71"
  },
  "sys_updated_on": "2021-05-04 11:47:54",
  "negation": "false",
  "sys_created_on": "2021-05-04 11:47:54",
  "location": "",
  "sys_created_by": "admin",
  "is_composition": "false",
  "sys_mod_count": "1",
  "operator": null,
  "security_tags": "",
  "malicious_attachment": "",
  "value": "81.69.35.30"
},
{
  "data": [
    {
      "type_id": 15,
      "published_at": "2021-05-04 16:27:54",
      "hash": "96ccba6f1872fe70028965da5b389ba0",
      "type": "IP Address",
      "id": 215845,
      "value": "81.69.35.30"
    }
  ],
  "total": 1
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY
sn_ti_observable.value	Indicator	indicator.value
sn_ti_observable.type.display_value	Indicator	indicator.type.name

Action Parameters

The Add Observable action offers the following configuration parameter:

PARAMETER	DESCRIPTION
Observable Finding	<p>Select the "finding" for the observable.</p> <p>Options include:</p> <ul style="list-style-type: none"> • Malicious (default) • Unknown

Operation: ServiceNow

Observable Finding

Malicious

Select what "finding" you want to give the observable

Run

Cancel

Add Ticket

This action adds (or updates) a ticket in ServiceNow (ie. Service Desk Incident, Security Incident, Security Task, or Security Case) based off of any TQ event. It will add the related indicators as related observables in ServiceNow.

PUT `https://<SNOW Host>/api/now/table/sn_si_incident, .../incident, .../sn_si_task, or .../sn_ti_case` to create the SNOW ticket

Sample Response:

```
{
  "upon_approval": "Proceed to Next Task",
  "sys_created_on": "2021-05-04 10:18:13",
  "knowledge": "false",
  "group_list": "",
  "urgency": "3 - Low",
  "location": "",
  "approval": "Not Yet Requested",
  "sys_domain": {
    "link": "https://ven04019.service-now.com/api/now/table/
sys_user_group/global",
    "display_value": "global"
  },
  "last_seen": "2021-05-04 10:18:15",
  "service_offering": "",
  "work_notes": "",
  "upon_reject": "Cancel all future Tasks",
  "calendar_duration": "",
  "watch_list": "",
  "user_input": "",
  "number": "SECC0001005",
  "state": "Open",
  "reassignment_count": "0",
  "comments_and_work_notes": "",
  "impact": "3 - Low",
  "active": "true",
  "company": "",
  "comments": "",
  "universal_request": "",
  "assignment_group": "",
  "delivery_plan": "",
  "due_date": "",
  "activity_due": "UNKNOWN",
  "sys_class_name": "Security Case",
  "case_type": "Campaign",
  "description": "<p>Test case</p>\n",
  "work_start": "",
  "priority": "4 - Low",
  "security_tags": "",
}
```

```

    "contact_type": null,
    "work_notes_list": "",
    "assigned_to": "",
    "route_reason": "",
    "sys_id": "d0e0e5a31bb7ec50cf41cbb5624bcbf8",
    "contract": "",
    "work_end": "",
    "sys_mod_count": "1",
    "follow_up": "",
    "sys_tags": "",
    "rating": "High",
    "additional_assignee_list": "",
    "sys_domain_path": "/",
    "close_notes": "",
    "short_description": "Test case",
    "sys_created_by": "admin",
    "escalation": "Normal",
    "opened_at": "2021-05-04 10:18:13",
    "expected_start": "",
    "skills": "",
    "order": "",
    "parent": "",
    "closed_at": "",
    "approval_history": "",
    "sys_updated_on": "2021-05-04 10:18:15",
    "business_service": "",
    "approval_set": "",
    "made_sla": "true",
    "correlation_display": "",
    "correlation_id": "",
    "delivery_task": "",
    "sla_due": "UNKNOWN",
    "sys_updated_by": "admin",
    "task_effective_number": "SECC0001005",
    "cmdb_ci": "",
    "business_duration": "",
    "closed_by": "",
    "time_worked": "",
    "opened_by": {
      "link": "https://ven04019.service-now.com/api/now/table/sys_user/6816f79cc0a8016401c5a33be04be441",
      "display_value": "System Administrator"
    }
  }
}

```



This action also uses `.../table/sn_ti_observable`, `.../sn_ti_m2m_task_observable`, and `.../table/sn_sec_cm_n_security_annotation` to create the observable, relate the observable, and add security annotations to the observable.

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH (TABLE.KEY)	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY
<code>ticket_type}.work_notes</code>	Event	<code>event.comments</code>
<code>{ticket_type}.description</code>	Event	<code>event.description</code>
<code>sn_ti_observable.value</code>	Indicator	<code>indicator.value</code>
<code>sn_ti_observable.type.display_value</code>	Indicator	<code>indicator.type.name</code>
<code>sn_sec_cm_n_security_annotation.annotation</code>	Indicator	<code>indicator.score</code>
<code>sn_sec_cm_n_security_annotation.annotation</code>	Indicator	<code>indicator.status</code>



Depending on the ticket type chosen (Service Desk Incident, Security Incident, Security Task, or Security Case), `ticket_type` will be substituted with `incident`, `sn_si_incident`, `sn_si_task`, or `sn_ti_case`.

Action Parameters

The Add Ticket action offers the following configuration parameter:

PARAMETER	DESCRIPTION
Select the Type of Ticket to Create in ServiceNow	Options include: <ul style="list-style-type: none"> Incident Security Incident Security Incident Response Task Security Case

Operation: ServiceNow



Select the type of ticket to create in ServiceNow

- ☐ Incident
- ☒ Security Incident
- ☐ Security Incident Response Task
- ☐ Security Case

Select the type of ticket to create in ServiceNow

Run

Cancel

Change Log

- **Version 1.1.1 rev-a**
 - Guide Update - Updated ServiceNow compatability versions.
- **Version 1.1.1**
 - Removed the HTML dependency as it is no longer used and also caused compatibility issues with the integration.
- **Version 1.1.0**
 - Added functionality to sync TQ events to ServiceNow along with their related indicators as ServiceNow Observables with Security Annotations and TQ comments as SNOW Work Notes
 - Sync the new SNOW tickets back to TQ as new event with attributes
- **Version 1.0.0**
 - Initial release