ThreatQuotient

ServiceNow Connector Guide

Version 2.4.0

Monday, February 24, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 703.574.9893

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.

Contents

Versioning

- Current integration version: 2.4.0
- Supported on ThreatQ versions: 4.3 or greater

Introduction

This integration connects ServiceNow to ThreatQ. It allows you to sync ServiceNow's default Service Desk incidents, as well as Security Incidents, Security Cases, and Observables (indicators) to ThreatQ. This integration can also add related objects in ThreatQ to ServiceNow.

Use Cases

- If a new incident (security, case, service desk, etc.) is detected in ServiceNow, it is added to ThreatQ with its ServiceNow number appended to the title.
    - If there are any parent or related incidents, they are added and related in ThreatQ.
    - Problems and Change requests are not added to ThreatQ.
- If an observable (indicator) is added to ServiceNow, it is added to ThreatQ.
- If there has been any new relationships created between incidents and other incidents or incidents and observables, those relationships are added to ThreatQ.
- If you add related indicators (observables) or events to a ThreatQ event (from ServiceNow), those related indicators/events are added to ServiceNow and related to the incident.
    - Related events sync only if they fall under the supported tables.
    - Related indicators sync only if they fall under the supported indicator types.
- ThreatQ attributes and metadata for Indicators are added to ServiceNow as an Observable's security annotations.
- Workflow comments/work_notes are not added to ThreatQ since they provide unneeded information and clutter the comments section in ThreatQ.
- Occasionally, ServiceNow does not update the sys_updated_on property of incidents immediately. The update can take up to thirty seconds.
- Due to syncing security annotations (indicator attributes), syncing requires more time. ServiceNow only supports one HTTP request per added security annotation at a time.

ThreatQ Event Types

The following are the ThreatQ event types that are created when installing the integration

- ServiceNow Service Desk Incident
- ServiceNow Security Incident
- ServiceNow Security Case

Permissions

This integration requires read/write access to the following tables:

Note: This list may vary depending on which options you have enabled in the ThreatQ UI configuration.

- incident
- sn_si_incident
- sn_ti_case
- sn_ti_m2m_task_observable
- sn_ti_m2m_case_task
- sn_ti_observable
- sn_ti_m2m_task_observable
- sys_journal_field (only before v2.0.2)

Supported Observable Types

The following are supported observable (indicator) types from ServiceNow. If you would like a type supported and it is not listed, please contact ThreatQ Support and we can add support for those types.

- IP Address (V4) -> IP Address
- Email address -> Email Address
- Unknown -> String
- SHA512 hash -> SHA-512
- Filename -> Filename
- File path -> File Path

- CIDR rule -> CIDR Block
- SHA1 hash -> SHA-1
- Registry key -> Registry Key
- Domain name -> FQDN
- MUTEX name -> Mutex
- URI -> URL Path
- SHA256 hash -> SHA-256
- MD5 hash -> MD5
- CVE number -> CVE
- URL -> URL
- Top-level domain name: FQDN

Installation

The connector can be installed from the ThreatQ integrations repository.

Perform the following steps to install the connector:

1. Install the connector using the following command:

```
pip install tq-conn-servicenow-*-py*-none-any.whl
```

   To install the connector from a .whl file, download the connector, and all of its dependencies, using the following command

```
pip download tq_conn_servicenow -d /tmp/distro/
```

   Copy the downloaded files, via SCP, to your ThreatQ instance. After completing that step, run the following command:

```
pip install tq_conn_servicenow-*-py*-none-any.whl
```

Once the connector is installed, a directory structure must be created for configuration, logs, and files.

   A driver called `tq-conn-servicenow` is installed.

2. Perform the following commands:

```
mkdir -p /etc/tq_labs/
mkdir -p /var/log/tq_labs/
```

3. Perform the initial run using one of the following commands based on your ServiceNow integration installation:

```
tq-conn-servicenow -v3 -ll /etc/tq_labs -c /var/log/tq_labs
tqServiceNow -v3 -ll /etc/tq_labs -c /var/log/tq_labs
tq-servicenow -v3 -ll /etc/tq_labs -c /var/log/tq_labs
```

4. Enter the following parameters when prompted:

Parameter	Description
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ. The recommended entry is **127.0.0.1.**

ThreatQ CID (Client ID)	This is the OAuth ID that can be found under a user's ThreatQ profile by navigating to the Systems gear icon > User Management and clicking the user.
Email Address	The username that you use to log into ThreatQ.
Password	The password associated with the username above.
Status	The default status for IoCs that are created by this integration. It is common to set this to **Active** but organization SOPs should be respected when setting this field.

The connector now appears on the integrations page in your ThreatQ instance. You still need to configure and enable the connector.

Configuration

Note: *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other connector-related credentials.*

To configure the feed:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the Category dropdown (optional).
3. Click on the connector to open its details page.
4. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
Host	Your ServiceNow hostname. The https:// prefix is optional.
Username	The ServiceNow username of the user interacting with ServiceNow/ThreatQ.
Password	The ServiceNow password of the user interacting with ServiceNow.
For the first run, how many days' worth of data do you want to pull?	This option specifies how many days in the past to pull information from. It must be a positive integer (no decimals).
Sync Service Desk Incidents?	*Yes* = Import Service Desk incidents from ServiceNow to ThreatQ. *No* = Ignore Service Desk incidents.
Synch Security Incidents?	*Yes* = Import Security Desk incidents from ServiceNow to ThreatQ. *No* = Ignore Security Desk incidents. **Note:** This option requires the Security Incident Response Plugin.

Sync Threat Intelligence?	*Yes* = Import Service Desk threat intelligence from ServiceNow to ThreatQ. This includes observables (indicators) and Security Cases (campaigns, adversaries, etc). *No* = Ignore Service Desk threat intelligence. **Note:** This option requires the Threat Intelligence Plugin.
ThreatQ User's Email/Username for Alerts	Setting this to an email or username of a ThreatQ user will allow the app to generate alerts on failure for that user in the ThreatQ UI.

5. Click **Save**.
6. Click the toggle switch, located above the *Additional Information* section, to enable it.

Configuring ServiceNow Plugins

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**.

Usage

Once the connector is installed to the ThreatQ UI and enabled, you will re-run the Initial Configuration command in order to kick off the integration.

Note: *Once the integration successfully completes, you will need to set up a CRON-job for it so it can run on a schedule.*

```
tq-conn-servicenow -ll /etc/tq_labs/ -c /var/log/tq_labs/ -v
<verbosity_level>
```

Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
`-h`, `--help`	Shows the help message and exits.
`-n, --name`	Sets the name for this connector. In some cases, it is useful to have multiple connectors of the same type executing against a single TQ instance. For example, the Syslog Exporter can be run against multiple target and multiple exports, each with their own name and configuration.
`-d, --no-differential`	If exports are used in this connector, this turns off the differential flag for the execution. This allows debugging and testing to be done on export endpoints without having to rebuild the exports after the test. THIS SHOULD NEVER BE USED IN PRODUCTION.
`-ll, --loglocation`	The path to the directory used to store your logs. The location should exist and be writable by the current user. A special value of 'stdout' means to log to the console (this happens by default).
`-c`	The path to the directory used to store your config file. This location must be readable and writable by the current user. If no config file is given, the current

	directory is used. This file also stores some information from each run of the connector (e.g. last run time, private oauth, etc).
`-v`	Sets the log verbosity. The default value is 1, log warnings. A value of 3 logs everything.
`--external-proxy, -ep`	Enables the use of a proxy to contact the Internet for the data required by this connector. This specifies an internet facing proxy, NOT a proxy to the TQ instance.
`--import`	Allows you to start the ServiceNow import function instead of running both import and export.
`--export`	Allows you to start the ServiceNow export function instead of running both import and export.
`-pt, --pid-timeout`	

Note: *All location-based options default to the current working directory if they are not provided. To find additional options and option descriptions, simply invoke the program with* `-h`.

CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector at the top of every hour.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

```
crontab -e
```

This will enable the editing of the crontab, using vi.

Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. To execute the connector at a scheduled frequency, you can configure a CRON entry to run the connector. Depending on how quickly you want updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

Hourly Example

```
0 * * * * tq-conn-servicenow -c /etc/tq_labs/ -ll
/var/log.tq_labs/ -v VERBOSITY_LEVEL
```

4. Save and exit cron.

Uninstalling the Connector

Run the following command to uninstall the connector:

```
sudo pip uninstall tq-conn-servicenow
```

Change Log

Version	Details
2.4.0	• Added functionality to allow the program to be run in both Python 2 and Python 3. • Alphabetized the imports in all .py files. • Removed requests from requirements.
2.3.2	• Fixed a bug that caused indicators without a type from ServiceNow to not be synced properly.
2.3.1	• Added more logging. • Fixed issues with syncing unicode from ServiceNow to ThreatQ. • Added the ability to get a notification in the ThreatQ UI when a failure in the ThreatQ app has occurred.
2.3.0	• Fixed issues that may arise with timezone props. • Improved comment handling. • Added pagination to fetch tickets. • Added PID timeout.
2.2.0	• Fixed issue with duplicates and updating new Tasks. • Added support for Security Incident Response Tasks. • Fixed issue with invalid observable link. • Fixed issue where child incidents were not related to the parent object in ThreatQ. • Fixed formatting when adding comments from workflow actions.

	• Added support for "updating" security tags that change. • Added the ability to run import/export separately.
2.1.2	• Fixed a bug that stopped data from being synced due to missing data. • Improved timezone handling and date formatting. • Fixed some instances of unicode characters not being synced to ThreatQ.
2.1.1	• Fixed an issue where an empty observable created in ServiceNow would break the sync to ThreatQ.
2.1.0	• Fixed several issues with syncing security annotations to ThreatQ. • Fixed several issues with creating comments in ThreatQ.
2.0.2	• Removed need to use sys_journal_field since only admins can access it. • Fixed comment differential.
2.0.1	• Created a fallback happened_at date so there are no crashes when sys_created_on is not available.
2.0.0	• Sync Service Desk Incidents. • Sync Threat Intelligence (Threat Intelligence Plugin). • Sync Security Incidents (Security Incident Response Plugin). • Sync relationships between incidents/cases and observables. • Add related indicators and events from ThreatQ to ServiceNow.

1.0.0	Initial Release