ThreatQuotient for ServiceNow Application

September 12, 2018

Version 2.1.0

11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
https://www.threatq.com/
Support: support@threatq.com
Sales: sales@threatq.com

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for ServiceNow Application attempts to mimic the ThreatQ Indicator and Event paradigm within ServiceNow.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for ServiceNow Application . Although it may be used as such, this document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and ServiceNow Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

1.4 Scope

This document only covers the implementation of the ThreatQuotient for ServiceNow Application to enable feeds to be passed to your ServiceNow Instance.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for ServiceNow Application	2.1.0	
ServiceNow	Jakarta or Earlier	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for ServiceNow Application into the managed estate:

- All ThreatQuotient equipment is online and in service.
- Infrastructure/transmission at all sites and between sites is in place to support the network traffic.
- All required firewall ports have been opened between ThreatQ and ServiceNow.
    - Port 443
- All equipment is powered from permanent power supplies.
- A clock source of sufficient accuracy is connected to the network and the network is using it as the primary clock source.

2 Implementation Overview

This document will show you how to install the ThreatQuotient for ServiceNow Application into ServiceNow.

2.1 Prerequisites

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

Ensure that ServiceNow's time zone is set to the time zone of the instance that the integration is running on.

If the time on both the ThreatQ instance and the ServiceNow Instance are not set to the same time and time zone, there could be issues with syncing incidents and indicators. This could increase the runtime as it will pick up incidents that may already be synced.

2.2 Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is strictly confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

3 ServiceNow Application Installation

3.1 Setting up the Integration

To install the ThreatQuotient for ServiceNow Application from the ThreatQuotient repository with YUM credentials, complete the following steps:

1. Install the ServiceNow application by using the following commands.

Figure 3: Installing from the ThreatQuotient Repository (Example Output)

```
[root@localhost]#
https://<USERNAME>:<PASSWORD>@extensions.threatq.com/threatq/integrations
tqServiceNow
You are using pip version 7.1.0, however version 10.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Collecting tqServiceNow
  Downloading https://extensions.threatq.com/threatq/integrations-
dev/+f/dcf/69db71fa56e7a/tqServiceNow-2.1.2-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): threatqsdk>1.6 in
/usr/lib/python2.7/site-packages (from tqServiceNow)
Requirement already satisfied (use --upgrade to upgrade): requests in
/usr/lib/python2.7/site-packages (from threatqcc>=1.3.0->tqServiceNow)
Requirement already satisfied (use --upgrade to upgrade): MarkupSafe in
/usr/lib64/python2.7/site-packages (from jinja2==2.8->threatqcc>=1.3.0-
>tqServiceNow)
Installing collected packages: tqServiceNow
Successfully installed tqServiceNow-2.1.2
You are using pip version 8.1.2, however version 18.0 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
[root@localhost]#
```

Once the application has been installed, A directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. See the example below:

Figure 4: Creating Integration directories (Example)

```
[root@localhost ~]# mkdir -p /opt/tq-integrations/SerNow/config
[root@localhost ~]# mkdir -p /opt/tq-integrations/SerNow/logs
[root@localhost ~]# cd /opt/tq-integrations/SerNow/
```

A driver called `tq-servicenow` or `tqservicenow` is installed.

2. Issue the following commands to initialize the integration.

Figure 5: Running the Integration (Example Output).

```
$> tqservicenow -c /opt/tq-integrations/SerNow/config -ll /opt/tq-
integrations/SerNow/logs/ -v3
ThreatQ Host: XXX.XXX.XXX.XXX
Client ID: <Client ID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured.  Set information in UI. xxxx-xx-xx xx:xx:xx -
tqServiceNow CRITICAL: Connector has been created, please use UI for final
configuration.
```

The driver will run once, where it will connect to the TQ instance and install the user interface component of the connector.

3.2 Configuring the connector

To edit the configuration, navigate to the **Incoming Feeds** page within ThreatQ, click the **ThreatQ Labs** tab, and then expand the **Feed Settings** for the **ServiceNow** section.

1. The following information will need to be entered as described below:
   - **Host:** This is your ServiceNow hostname. 'https://' is optional.
   - **Username:** Enter the ServiceNow username of the user that will interact with ServiceNow and ThreatQ.
   - **Password**: Password for the above username
   - **ThreatQ Hostname/IP:** ThreatQ Hostname or IP
   - **For the first run, how many days' worth of data do you want to pull?:** This option will determine how many days in the past to pull information from. It must be a positive integer (*no decimals*).
   - **Sync Service Desk Incidents?:** Setting this to 'Yes' will import Service Desk incidents from ServiceNow to ThreatQ. Setting it to 'No' will ignore them.
   - **Sync Security Incidents?:** Setting this to 'Yes' will import Security incidents from ServiceNow to ThreatQ. Setting it to 'No' will ignore them. You must have the 'Security Incident Response' plugin for this to work.
   - **Sync Threat Intelligence?:** Setting this to 'Yes' will import Service Desk incidents from ServiceNow to ThreatQ. Setting it to 'No' will ignore them. This includes observables (indicators) and Security Cases (campaigns, adversaries, etc.). You must have the 'Threat Intelligence' plugin installed for this to work.
   - **Sync Security Annotations Immediately?:** This option applies to when adding Observables from ServiceNow to ThreatQ as indicators. If this option is set to 'Yes', adding indicators to ThreatQ will take more time. Significantly more time if there are many indicators to sync (>1k). If set to 'No', the ThreatQ Link annotation will not be added until the observable is updated in ServiceNow

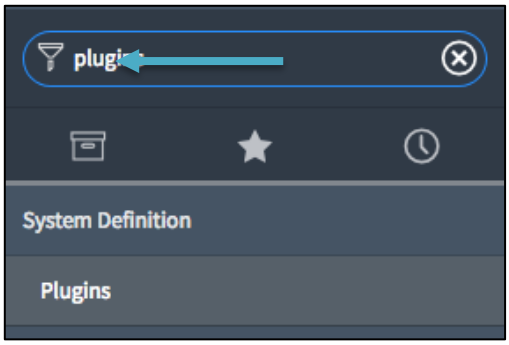
Figure 6: ThreatQ UI Configuration

3.1 Configuring ServiceNow Plugins

ServiceNow requires three plugins: **Threat Intelligence**, **Vulnerability Response**, and **Security Incident Response**. They must be installed in this order. To install the plugins after logging into your ServiceNow instance, follow these steps:

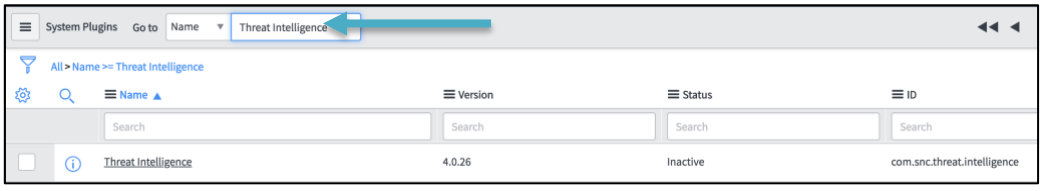
1. From the filter navigator, search for **Plugins**.

Figure 7: ServiceNow Search Plugins



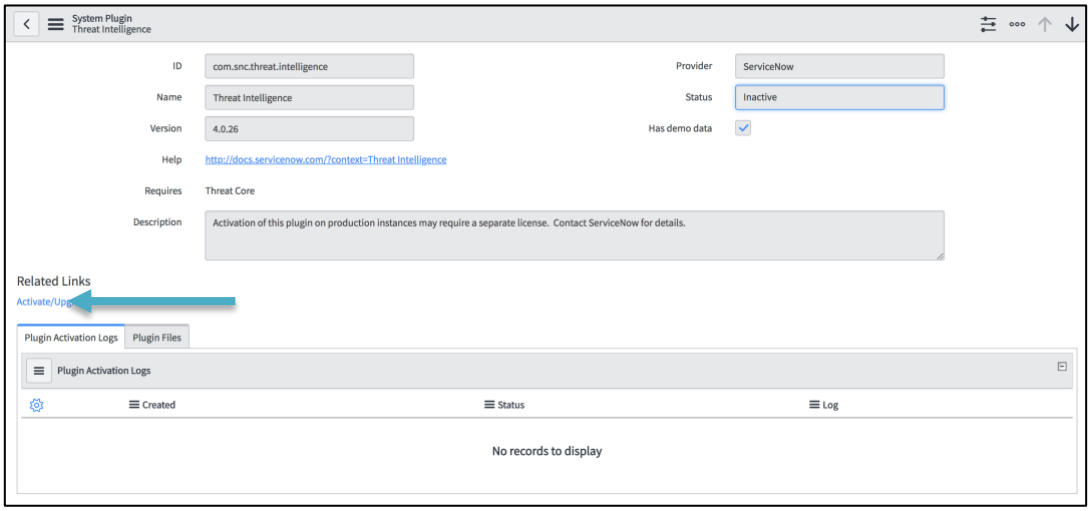
2. Click **Plugins**.
3. Search for each of the plugins in turn, select it and you will navigate to the plugin page. (Threat Intelligence is used as an example).

Figure 8: ServiceNow Search Result



4. Click **Threat Intelligence**.
5. Under related links, select **Activate/Update**.

Figure 9: ServiceNow Activate Plugin



6. A progress bar will appear, showing the progress of the plugin activation.

Figure 10: ServiceNow Plugin Activation Progress

7. The modal will update to tell you the activation was complete. You can the press the 'View Plugin List' button and repeat these steps until all plugins are installed. Once the final plugin is installed, you can select the **Close & Reload Form** button.

Figure 11: ServiceNow Plugin Activation Success

3.1.1 Setting Up the CRONJOB

1. Login via a CLI terminal session to your ThreatQ host.
2. Input the commands below.

Figure 12: Command Line Crontab 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. Input the commands below – this example shows every **4 Hours**.

Figure 13: Command Line Crontab ServiceNow Command

```
0 */4 * * * $> tqServiceNow -c /path/to/config/directory  -ll
/path/to/logs/directory -v3
```

To run this script on a reoccurring basis, use CRON or some other on system schedule. CRON is shown here.

For further reference, see the ThreatQ Help Center.

Appendix B: Acronym Listing or Glossary

Term	Definition
TQIS	ThreatQ Integration Server
CID	Client Identity
App	Application
SDK	Software Development Kit
SCP	Secure Copy Protocol
HTTP	HyperText Transfer Protocol
CLI	Command Line Interface
VI	visual instrument (vi is a screen-oriented text editor)
IP	Internet Protocol
SSL	Secure Sockets Layer
UI	User Interface

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.