

ThreatQuotient



ServiceNow App Guide

Version 1.0.9 rev-a

January 11, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

- Support 4
- Versioning..... 5
- Introduction 6
- Prerequisites 7
- Installation..... 8
- Configuration 9
- Usage..... 11
 - Creating a Security Incident..... 11
 - Accessing Threat Lookup Results 14
 - Threat Lookup Example 14
 - Viewing Observable Enrichment Results 15
 - Enrichment Details Example 16
- FAQs 17
- Change Log..... 18

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 © 2022 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.

Versioning

Current integration version: 1.0.9

Introduction

The ServiceNow app is an integration that lives within the ServiceNow Marketplace and enables users to query the ThreatQ directly from the ServiceNow UI. This application has been certified by ServiceNow and is developed within their platform framework.

The current integration between ThreatQ and ServiceNow enables users to import ServiceNow Observables/Security Incidents into ThreatQ as Indicators/Security Events. This process is initiated by a ThreatQ custom connector and the data flow for this integration is one-sided and flows from ServiceNow → ThreatQ.

This new integration is an inverse of the existing capabilities and is initiated by ServiceNow. The data flow for this application is in the opposite direction and flows from ThreatQ → ServiceNow.

	THREATQ SERVICENOW CONNECTOR(EXISTING)	SERVICENOW APPLICATION (NEW)
Action Initiator	ThreatQ	ServiceNow
Data Flow	ServiceNow -> ThreatQ	ThreatQ -> ServiceNow



This integration is not meant to replace the existing ThreatQ custom connector implementation but rather to complement existing capabilities. ServiceNow users can now query the ThreatQ dataset directly from the ServiceNow platform UI.

Prerequisites

The ServiceNow App integration requires you to enter your **OAuth Client ID** and **OAuth Client Secret** when [configuring](#) the integration. You can generate both using the steps below.



You can also use the steps below to view existing credentials by using an existing integration name for the `--name` flag.

1. SSH to your ThreatQ installation.
2. Navigate to the api directory:

```
<> cd /var/www/api
```

3. Create a OAuth Client ID and Secret using the following command:

```
<> php artisan threatq:oauth2-client --name <ServiceNowApp>
```

Example Output:

```
php artisan threatq:oauth2-client --name ServiceNowApp
session_timeout_minutes: 1440
name: ServiceNowApp
type: private
client_id: njnjm2qxmdjy2flmzkxmziyzgy5n2uy
client_secret: NmFkY2FiMTZhY2UwYjA5ZGFjZjUyOGQ2ZDhjOWRlMzYwOTFiNjcxNzVkNTE4NmU5
updated_at: 2022-01-06 02:03:04
created_at: 2022-01-06 02:03:04
id: 19
```



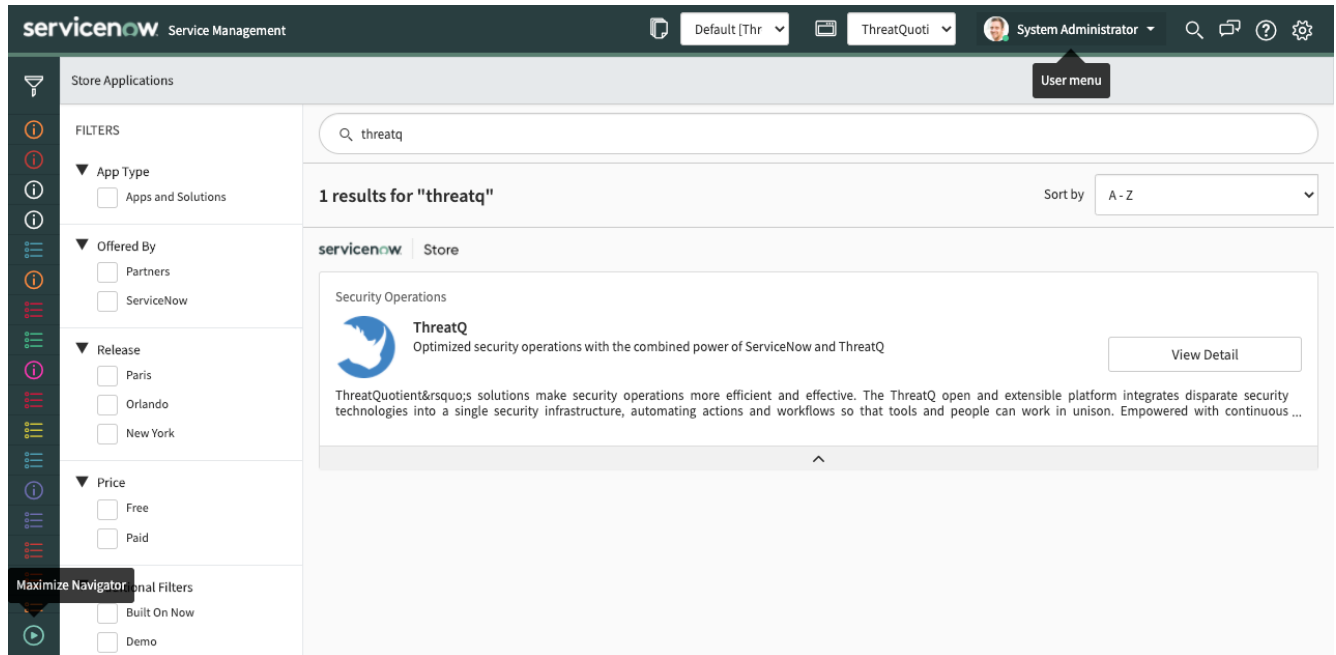
Be sure to generate **Private Type** credentials. **Public Types** will only generate Client ID and not a Client Secret. You can add a `--type private` flag to the command to ensure a **Private Type** is generated.

4. Copy the Client ID and Secret to a safe location to use when [configuring](#) integration.

Installation

Within the ServiceNow interface:

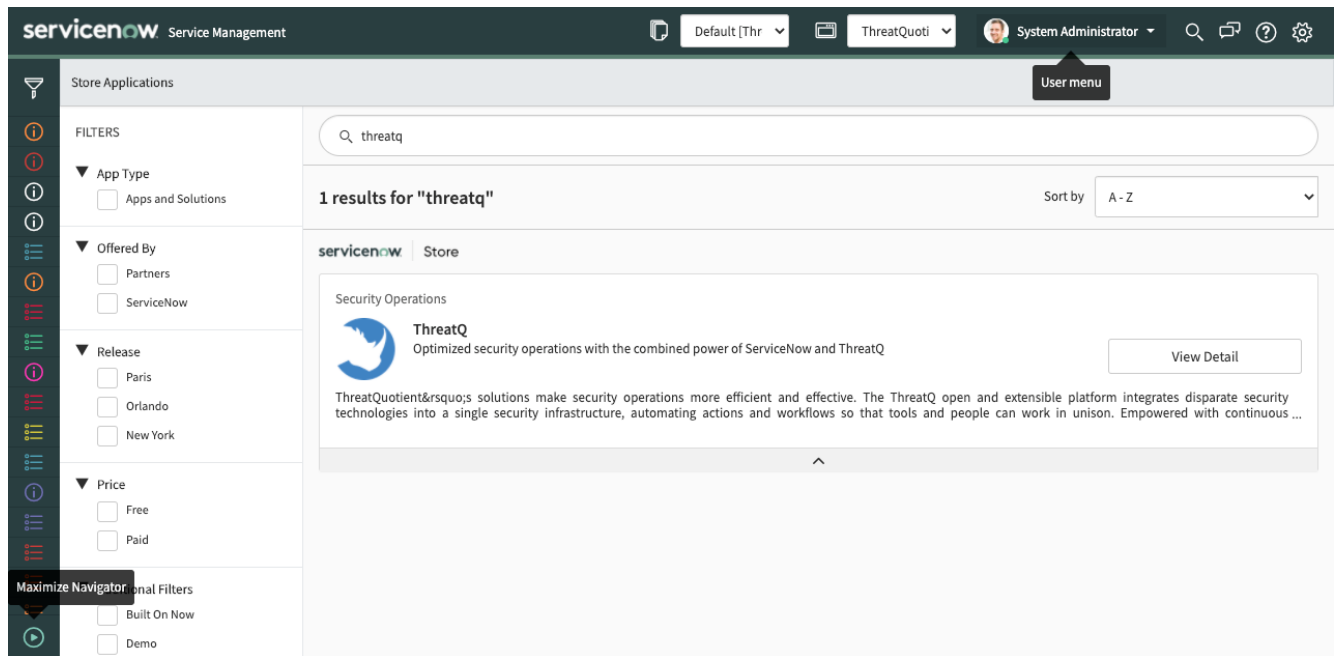
1. Use the Filter navigator and navigate to **System Applications - ServiceNow Store**.
2. Search for **ThreatQ** within the Store Application and then click the **Install** button.



Configuration

Within the ServiceNow interface:

1. Click **Security Operations >> Integration Configuration** after the application has been installed.



2. Add your OAuth configuration:

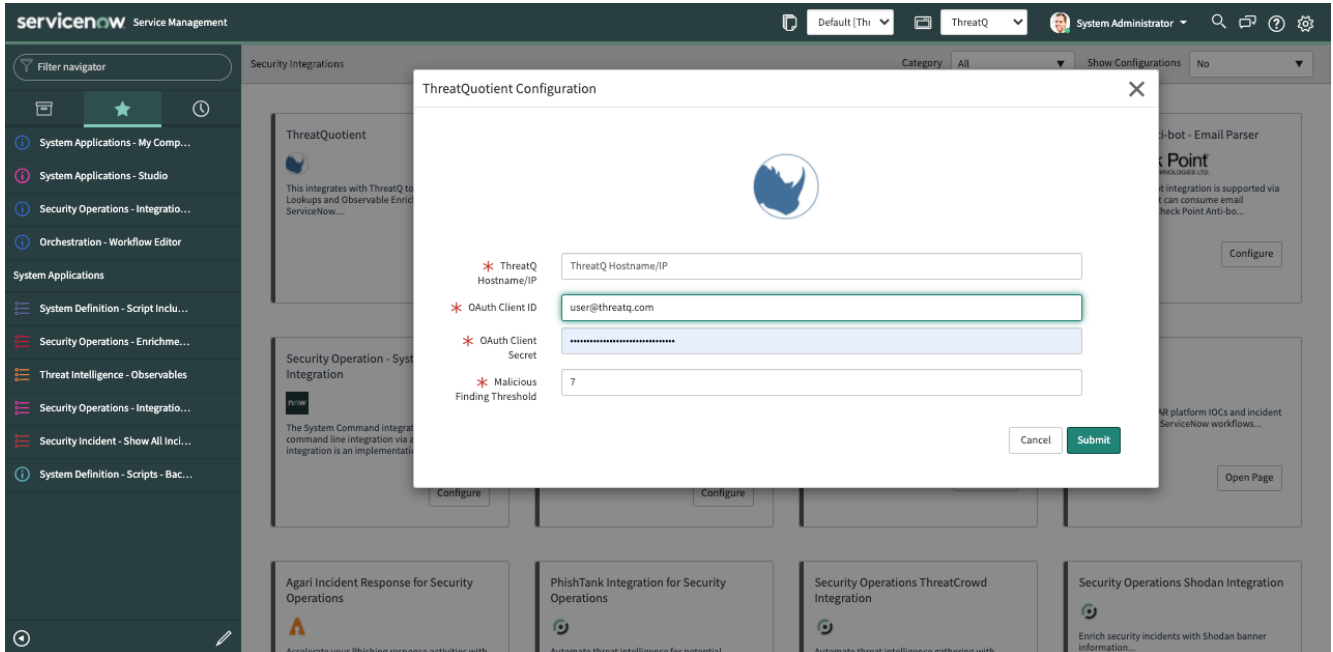
FIELD	DESCRIPTION
ThreatQ Hostname	Your ThreatQ instance hostname or IP.
OAuth Client ID	This is the OAuth Client ID you generated for use with this integration. See the Prerequisites chapter for steps on how to generate or retrieve your OAuth Client ID for this integration.
OAuth Client Secret	This is the OAuth Client Secret associated with the OAuth Client ID above. See the Prerequisites chapter for steps on how to generate or retrieve your OAuth Client Secret for this integration.

FIELD

DESCRIPTION

Malicious
Finding
Threshold

Enter your threshold value in this field.



The screenshot shows the ServiceNow interface with a 'ThreatQuotient Configuration' dialog box open. The dialog box has a title bar with a close button. Inside, there is a ThreatQuotient logo at the top. Below the logo, there are four configuration fields, each preceded by a red asterisk indicating a required field:

- ThreatQ Hostname/IP**: An empty text input field.
- OAuth Client ID**: A text input field containing the value 'user@threatq.com'.
- OAuth Client Secret**: A text input field containing a masked string of asterisks.
- Malicious Finding Threshold**: A text input field containing the value '7'.

At the bottom right of the dialog box, there are two buttons: 'Cancel' and 'Submit'. The 'Submit' button is highlighted in green.

3. Click on **Submit**.

Usage

The following section will describe the steps required to create a security incident, access threat lookup results, and view observable enrichment results.

Creating a Security Incident

1. Create a new Security Incident.

The screenshot displays the ServiceNow Security Incidents interface. The left sidebar contains a filter navigator with various system and security-related categories. The main content area shows a table of security incidents. The table has columns for Number, Risk score, Priority, Configuration item, Assigned to, Assignment group, Short description, and State. The incidents listed are all in 'Draft' state and have a risk score of 47 and priority of 4-Low. The descriptions include 'security incident test', 'testing FQDN', 'Testing recently queried observables', 'Last test before publishing', 'testing out new observables', 'Testing using the enrich observable capability', 'Testing automatic threat lookup', 'test tes test', 'Test incident', and 'Incidents with observables that don't exist in ThreatQ'. The bottom right corner shows a response time bar and a status indicator.

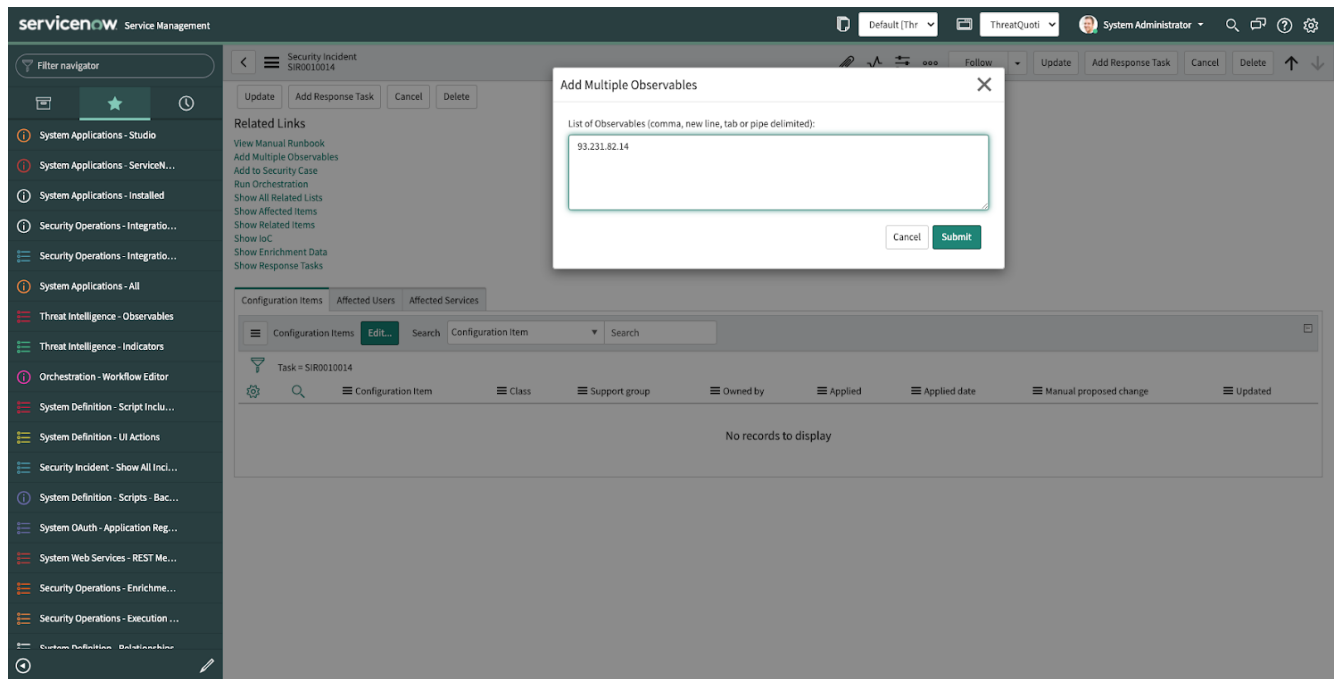
Number	Risk score	Priority	Configuration item	Assigned to	Assignment group	Short description	State
SIR0010002	47	4-Low	(empty)	(empty)	Security Incident Assignment	security incident test	Draft
SIR0010012	47	4-Low	(empty)	(empty)	Security Incident Assignment	testing FQDN	Draft
SIR0010011	47	4-Low	(empty)	(empty)	Security Incident Assignment	Testing recently queried observables	Draft
SIR0010010	47	4-Low	(empty)	(empty)	Security Incident Assignment	Last test before publishing	Draft
SIR0010008	47	4-Low	(empty)	(empty)	Security Incident Assignment	testing out new observables	Draft
SIR0010007	47	4-Low	(empty)	(empty)	Security Incident Assignment	Testing using the enrich observable capability	Draft
SIR0010006	47	4-Low	(empty)	(empty)	Security Incident Assignment	Testing automatic threat lookup	Draft
SIR0010005	47	4-Low	(empty)	(empty)	Security Incident Assignment	test tes test	Draft
SIR0010004	47	4-Low	(empty)	(empty)	Security Incident Assignment	Test incident	Draft
SIR0010013	47	4-Low	(empty)	(empty)	Security Incident Assignment	Incidents with observables that don't exist in ThreatQ	Draft

2. Give the Security Incident a short description.

The screenshot shows the ServiceNow 'Security Incident' form in the 'Draft' state. The left sidebar contains a 'Filter navigator' with various system and security-related links. The main form area has a progress bar at the top with stages: Draft, Analysis, Contain, Eradicate, Recover, Review, and Closed. The 'Draft' stage is active. The form fields are organized into two columns. The left column includes 'Number' (SIR0010014), 'Requested by', 'Configuration item', 'Affected user', 'Location', 'Category' (set to '-- None --'), and 'Subcategory' (set to '-- None --'). The right column includes 'Opened' (2020-08-13 06:59:09), 'State' (Draft), 'Substate' (set to '-- None --'), 'Source' (set to '-- None --'), 'Alert Sensor' (set to '-- None --'), 'Risk score', 'Risk score override' (checkbox), 'Business impact' (3 - Non-critical), 'Priority' (4 - Low), 'Assignment group', and 'Assigned to'. Below these fields is a 'Short description' field containing the text 'This is a demo incident'. At the bottom, there is a 'Knowledge results' section showing 'No matching results found for This is a demo incident'.

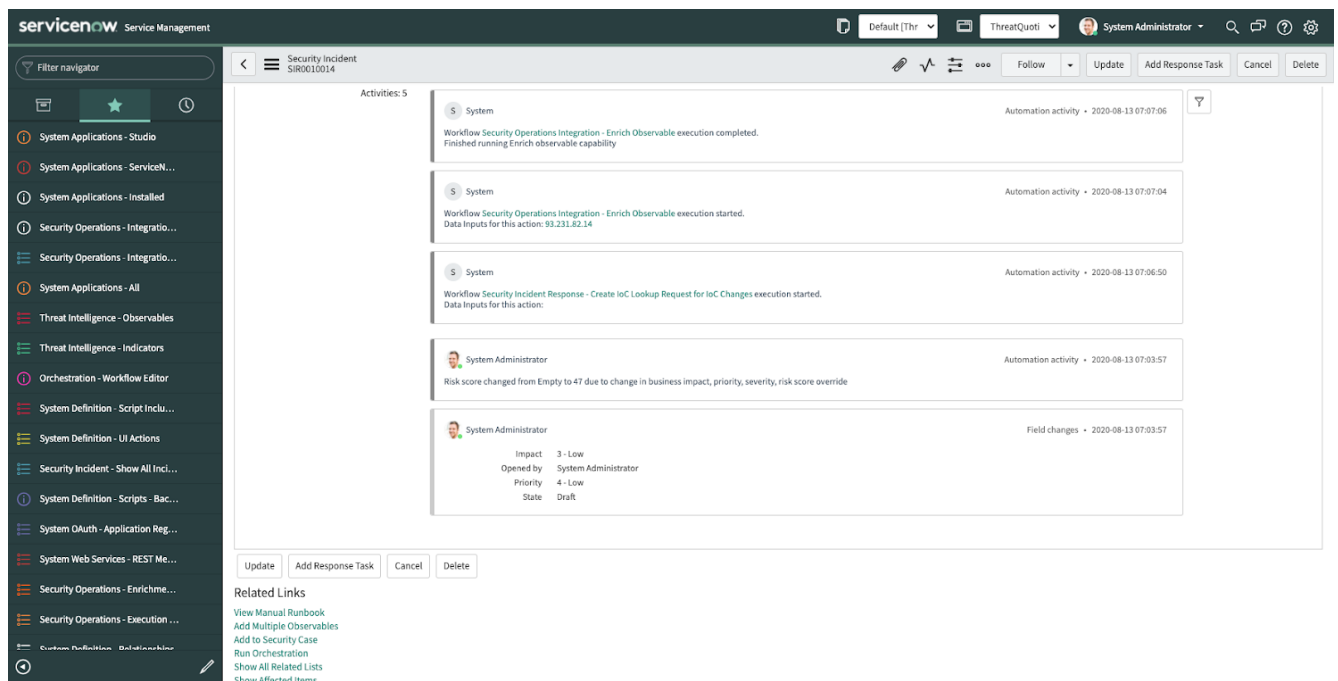
3. Add observables to the Security Incident.

The screenshot shows the ServiceNow 'Security Incident' form for incident SIR0010014. The top navigation bar includes 'Update', 'Add Response Task', 'Cancel', and 'Delete' buttons. Below the navigation bar is a 'Related Links' section with links such as 'View Manual Runbook', 'Add Multiple Observables', 'Add to Security Case', 'Run Orchestration', 'Show All Related Lists', 'Show Affected Items', 'Show Related Items', 'Show IoT', 'Show Enrichment Data', and 'Show Response Tasks'. The 'Configuration Items' tab is selected, showing a table with columns: Configuration Item, Class, Support group, Owned by, Applied, Applied date, Manual proposed change, and Updated. The table is currently empty, displaying 'No records to display'.



4. Click on Submit and wait for automatic threat lookup activity to complete.

You can see the new observables when you click **Show IoC**.



Accessing Threat Lookup Results

1. Click Threat Lookup Results to see if the IOC was found in ThreatQ.

The screenshot shows the ServiceNow Security Incident interface for incident SIR0010014. The 'Threat Lookup Results' tab is selected, displaying a table with one row of results for the observable 93.231.82.14. The table columns include Value, Observable type, Context, Incident count, and Updated. The 'Value' column contains the IP address 93.231.82.14, and the 'Updated' column shows the date 2020-08-13 07:06:04.

Value	Observable type	Context	Incident count	Updated
93.231.82.14	IP address (V4)	(empty)	2	2020-08-13 07:06:04

Threat Lookup Example

The screenshot shows the ServiceNow Security Incident interface for incident SIR0010014. The 'Threat Lookup Results' tab is selected, displaying a table with two rows of results for the observable 93.231.82.14. The table columns include Observable, Integration vendor, Finding, Result value, Details, Source Engine, Engine version, and Retrieval date. The 'Integration vendor' is ThreatQuotient, and the 'Result value' is 'Observable was found in ThreatQ'. The 'Retrieval date' for the first row is 2020-08-13 07:07:05, and for the second row is 2020-08-10 11:09:55.

Observable	Integration vendor	Finding	Result value	Details	Source Engine	Engine version	Retrieval date
93.231.82.14	ThreatQuotient	Unknown	Observable was found in ThreatQ	Status: Active Create Date: 2020-08-09 1...	ThreatQ	4.39.0-850	2020-08-13 07:07:05
93.231.82.14	ThreatQuotient	Unknown	Observable was found in ThreatQ	Status: Active Create Date: 2020-08-09 1...	ThreatQ	4.39.0-850	2020-08-10 11:09:55

Viewing Observable Enrichment Results

1. Click **Observable Enrichment Results** to see the IOC details.

The screenshot displays the ServiceNow ThreatQuotient interface. On the left is a sidebar with a 'Filter navigator' and a list of system applications. The main content area shows the 'Threat Lookup Result' for the observable '93.231.82.14'. The interface is divided into several sections:

- Observable:** 93.231.82.14
- Finding:** Unknown
- First found:** 2020-08-09 11:39:45
- Security tags:**
- External link:** <https://servicenowint.threatq.com/indicators/8361/details>
- Details:**
 - Status: Active
 - Create Date: 2020-08-09 18:39:45
 - Last Updated: 2020-08-09 18:39:45
 - Sources: www.dan.me.uk Tor Node List
- Result value:** Observable was found in ThreatQ
- Raw data:**

```
[{"total":1,"data":[{"id":"8361","type":"ip","status_id":15,"class":"network","hash":"4eeef1dd74b56209aa43bc896a3467d","value":"93.231.82.14","description":null,"last_detected_at":null,"expires_at":null,"expired_at":null,"expires_needs_calc":false,"expires_calculated_at":"2020-08-09 18:40:22","created_at":"2020-08-09 18:39:45","updated_at":"2020-08-09 18:39:45","touched_at":"2020-08-09 18:39:47","attributes":[{"id":"73991","indicator_id":"8361","attribute_id":"7","value":"9030","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"Directory Port","attribute":{"id":"7","name":"Directory Port","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"id":"73992","indicator_id":"8361","attribute_id":"5","value":"Michael","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"Contact","attribute":{"id":"5","name":"Contact","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"id":"73993","indicator_id":"8361","attribute_id":"8","value":"0x0EAD0BEEF","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"TOR Name","attribute":{"id":"8","name":"TOR Name","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"id":"73994","indicator_id":"8361","attribute_id":"9","value":"9001","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"Router Port","attribute":{"id":"9","name":"Router Port","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"id":"73995","indicator_id":"8361","attribute_id":"6","value":"FRD","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"Flags","attribute":{"id":"6","name":"Flags","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"id":"73996","indicator_id":"8361","attribute_id":"11","value":"","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"Uptime","attribute":{"id":"11","name":"Uptime","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"id":"73997","indicator_id":"8361","attribute_id":"10","value":"for 0.4.3.6","created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","touched_at":"2020-08-09 18:39:47","name":"Version","attribute":{"id":"10","name":"Version","created_at":"2020-08-07 18:36:01","updated_at":"2020-08-07 18:36:01"},"sources":[{"id":"12","type":"connectors","reference_id":"37","name":"www.dan.me.uk Tor Node List","tip_id":null,"created_at":"2020-08-09 18:39:47","updated_at":"2020-08-09 18:39:47","published_at":null,"pivot":{"indicator_id":"8361","source_id":"12","id":"23277","creator_source_id":"12"},"score":{"indicator_id":"8361","generated_score":"0.00","manual_score":null,"score_config_hash":"7f8b888a2d3b4623306527aa7568ca76973a96","created_at":"2020-08-09 18:39:45","updated_at":"2020-08-09 18:39:45"},"status":{"id":"1","name":"Active","description":"Poses a threat and is being exported to detection"}]}
```

Enrichment Details Example

The screenshot displays the ServiceNow ThreatQuotient interface. The top navigation bar includes the 'servicenow' logo, 'Service Management', and user information for 'System Administrator'. The left sidebar contains a 'Filter navigator' and a list of system applications and security operations. The main content area shows the 'Security Incident' details for 'SIR0010014'. The 'Related Links' section lists various actions like 'View Manual Runbook', 'Response Workflow', and 'Add to Security Case'. The 'Observable Enrichment Results' tab is active, displaying a table with two rows of enrichment data. The table has columns for 'Integration vendor', 'Observable', 'Summary', and 'Retrieval date'. Both rows show 'ThreatQuotient' as the vendor and '93.231.82.14' as the observable, with a summary of 'Directory Port: 5030 Contact: Michael TO...' and retrieval dates of '2020-08-13 07:07:06' and '2020-08-10 11:09:55' respectively. A pagination bar at the bottom indicates '1 to 2 of 2' results.

servicenow Service Management

Default [Thr] ThreatQuoti System Administrator

Filter navigator

System Applications - Studio

System Applications - ServiceN...

System Applications - Installed

Security Operations - Integratio...

Security Operations - Integratio...

System Applications - All

Threat Intelligence - Observables

Threat Intelligence - Indicators

Orchestration - Workflow Editor

System Definition - Script Inclu...

System Definition - UI Actions

Security Incident - Show All Inci...

System Definition - Scripts - Bac...

System OAuth - Application Reg...

System Web Services - REST Me...

Security Operations - Enrichme...

Security Operations - Execution ...

Custom Definition Relationship

Security Incident SIR0010014

Related Links

- View Manual Runbook
- Response Workflow
- Add Multiple Observables
- Add to Security Case
- Run Orchestration
- Show All Related Lists
- Show Affected Items
- Show Related Items
- Show IoC
- Show Enrichment Data
- Show Response Tasks

Running Processes Running Services Network Statistics Domain Lookups Firewall Logs Compromised User Info CI Enrichment Observable Enrichment Results (2)

Observable Enrichment Results

Integration vendor Observable Summary Retrieval date

ThreatQuotient	93.231.82.14	Directory Port: 5030 Contact: Michael TO...	2020-08-13 07:07:06
ThreatQuotient	93.231.82.14	Directory Port: 5030 Contact: Michael TO...	2020-08-10 11:09:55

Actions on selected rows...

1 to 2 of 2

FAQs

QUESTION	OUTCOME
Does this integration support on-prem ThreatQ installations?	Possible, ServiceNow needs to be able to directly communicate with ThreatQ. ThreatQ will add support for the ServiceNow MID Server in future releases. This will enable ServiceNow to indirectly access applications platforms that are hosted behind a firewall. However, ServiceNow MID Server currently does not support OAuth.
Can this integration create indicators within ThreatQ?	Currently, the integration only supports querying ThreatQ for data and then sending the data to ServiceNow for analysis. In Phase 2 of this project, the goal is to become bi-directional and allow data to be ingested into ThreatQ by ServiceNow.
Does this replace the current ServiceNow custom connector?	No, currently, the two implementations are complementary.

Change Log

- **Version 1.0.9 - reva**
 - Updated [Configuration](#) chapter details regarding OAuth Client ID and OAuth Client Secret.
 - Added new [Prerequisites](#) with steps on generating or retrieving OAuth Client ID and OAuth Client Secret.
- **Version 1.0.9**
 - Initial Release