

# ThreatQuotient



## ServiceNow App Guide

Version 1.1.0

September 27, 2022

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

- Integration Details..... 5
- Introduction ..... 6
- Prerequisites..... 7
- Installation..... 8
- Configuration ..... 9
- Usage..... 11
  - Creating a Security Incident..... 11
  - Accessing Threat Lookup Results ..... 14
  - Threat Lookup Example ..... 15
  - 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](mailto: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 App Version	1.1.0
Compatible with ThreatQ Versions	>=4.0.0
Validated	Quebec, Rome, San Diego, Tokyo
Support Tier	ThreatQ Supported
ThreatQ Marketplace	<a href="https://marketplace.threatq.com/details/servicenow-app">https://marketplace.threatq.com/details/servicenow-app</a>

# 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
```

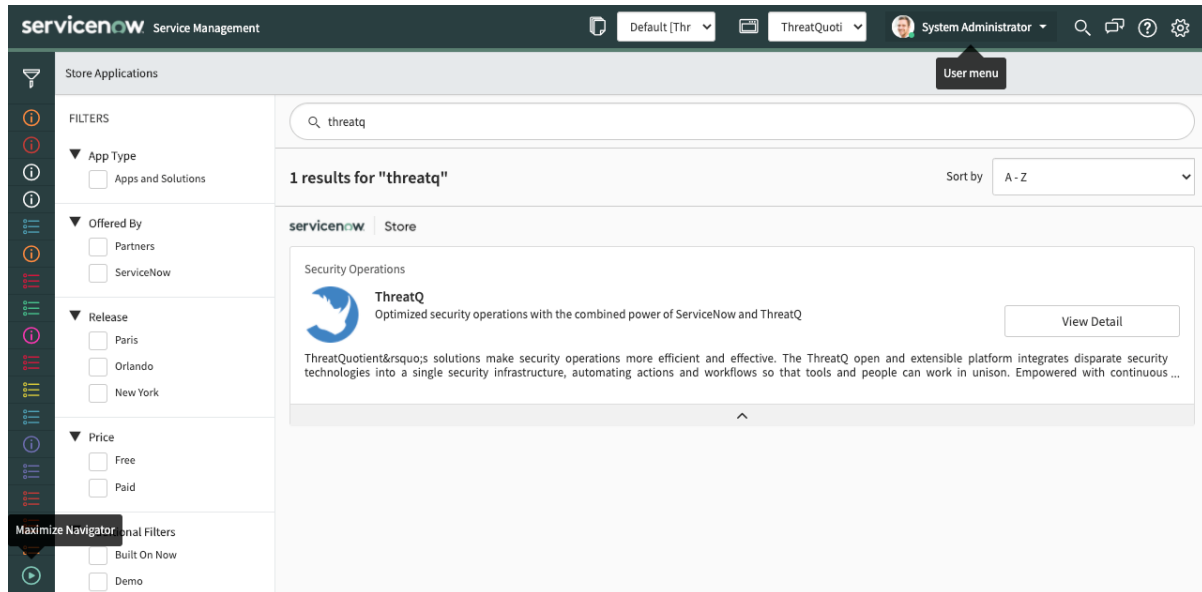
Be sure to generate **Private Type** credentials. **Public Types** will only generate Client ID and not a Client Secret. You can add a `--type private` flag to the command to ensure a **Private Type** is generated.

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.

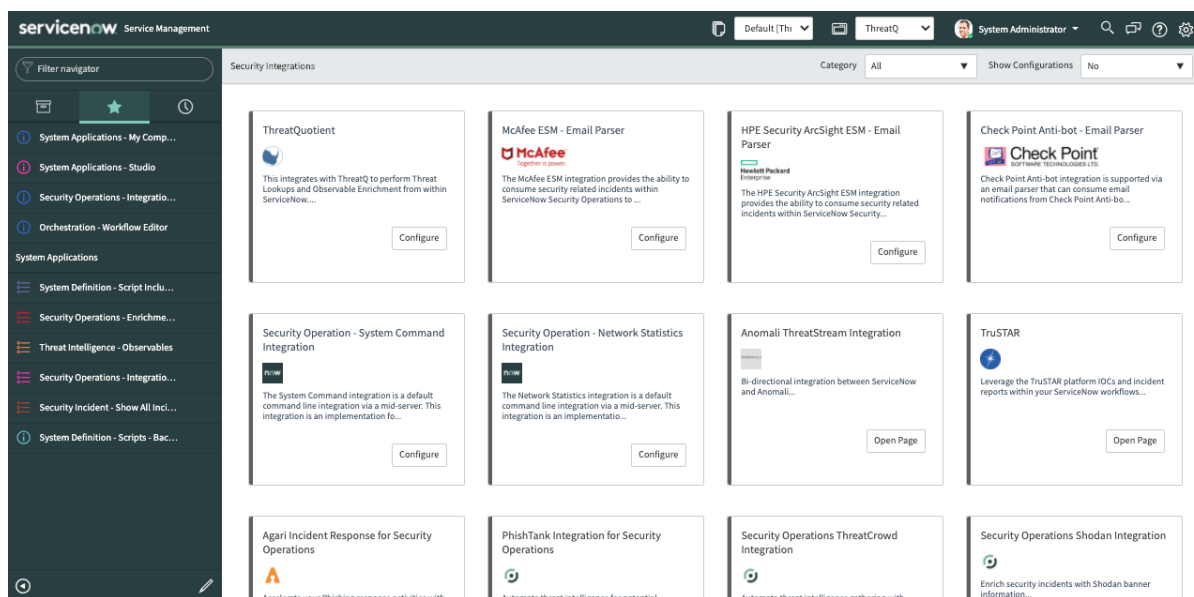




# Configuration

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 <a href="#">Prerequisites</a> 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 <a href="#">Prerequisites</a> chapter for steps on how to generate or retrieve your OAuth Client Secret for this integration.

## FIELD

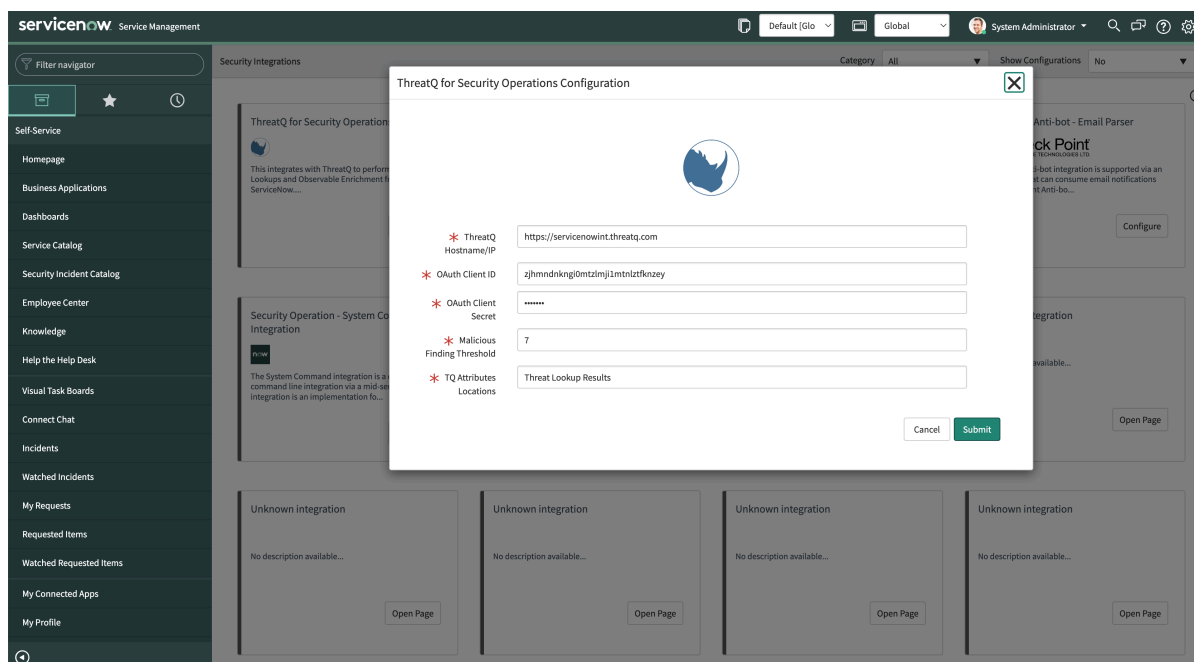
## DESCRIPTION

### Malicious Finding Threshold

Enter the threshold value based off of which indicators having a score equal to or higher than this number will be labeled as malicious.

### TQ Attribute Locations

Specify the table where you want to save each indicator's attributes. Options include either Threat Lookup Results or Observable Enrichment Results.



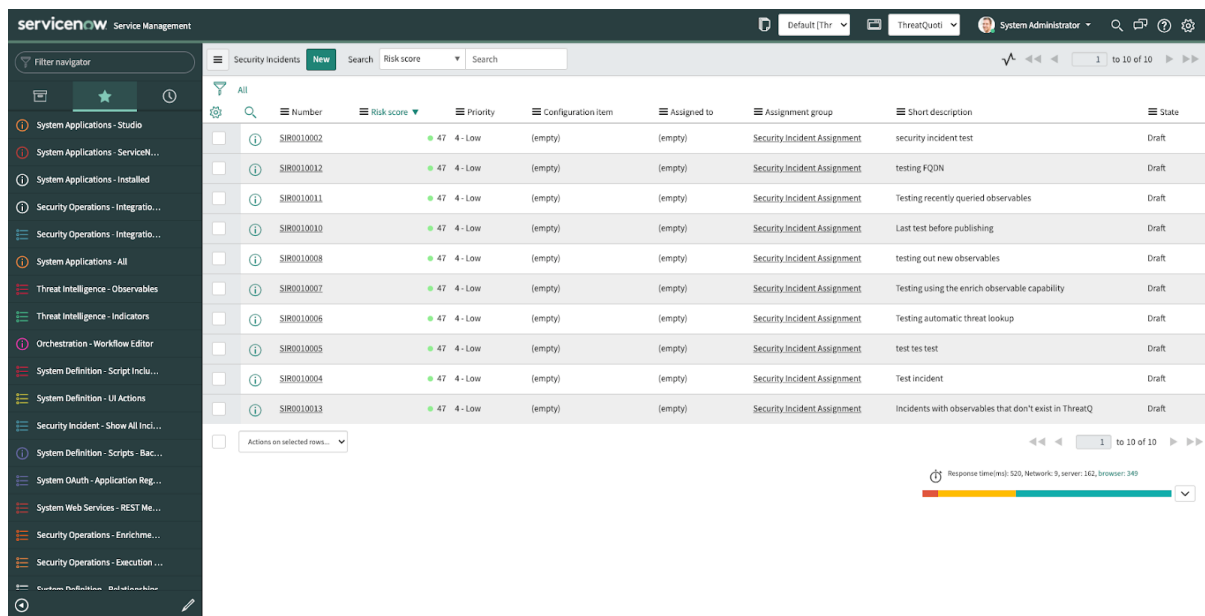
3. Click on **Submit**.

# 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 shows the ServiceNow Security Incidents interface. The left sidebar contains a filter navigator with various system applications and security operations. The main content area displays 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 FQON', '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'.

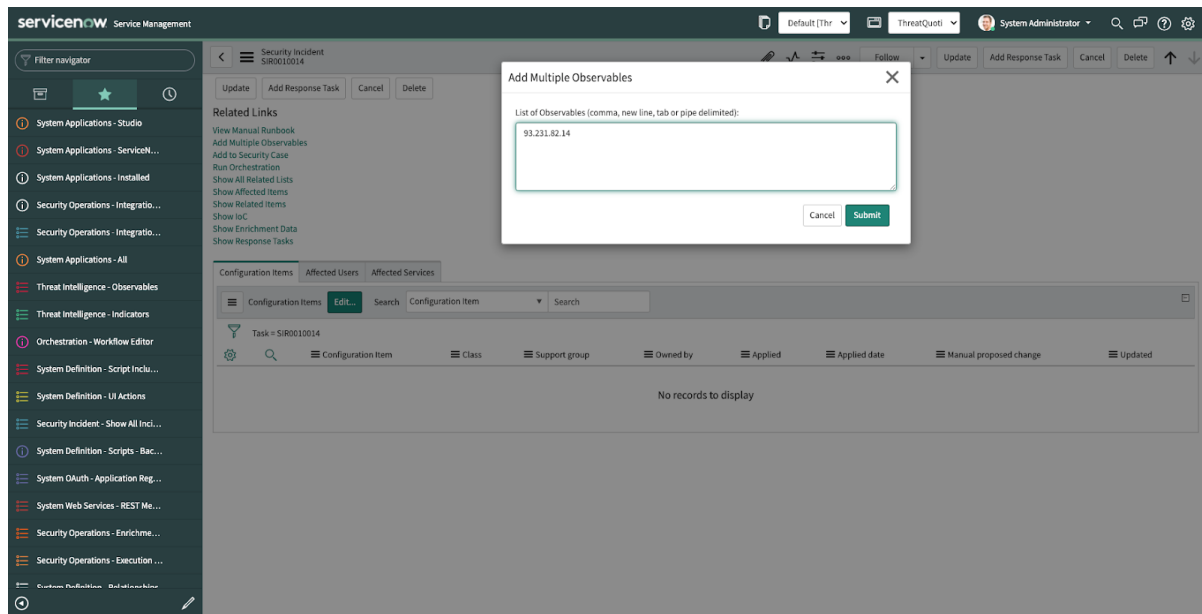
Number	Risk score	Priority	Configuration item	Assigned to	Assignment group	Short description	State
SIR0010002	47	4-Low	(empty)	(empty)	Security Incident Assignment	security incident test	Draft
SIR0010012	47	4-Low	(empty)	(empty)	Security Incident Assignment	testing FQON	Draft
SIR0010011	47	4-Low	(empty)	(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 form includes fields for Number (SIR0010014), Requested by, Configuration item, Affected user, Location, Category, and Subcategory. On the right, there are fields for Opened (2020-08-13 06:59:09), State (Draft), Substate, Source, Alert Sensor, Risk score, Risk score override, Business impact (3 - Non-critical), Priority (4 - Low), Assignment group, and Assigned to. A 'Short description' field contains the text 'This is a demo incident'. Below the form, a 'Knowledge results' section shows 'No matching results found for This is a demo incident'.

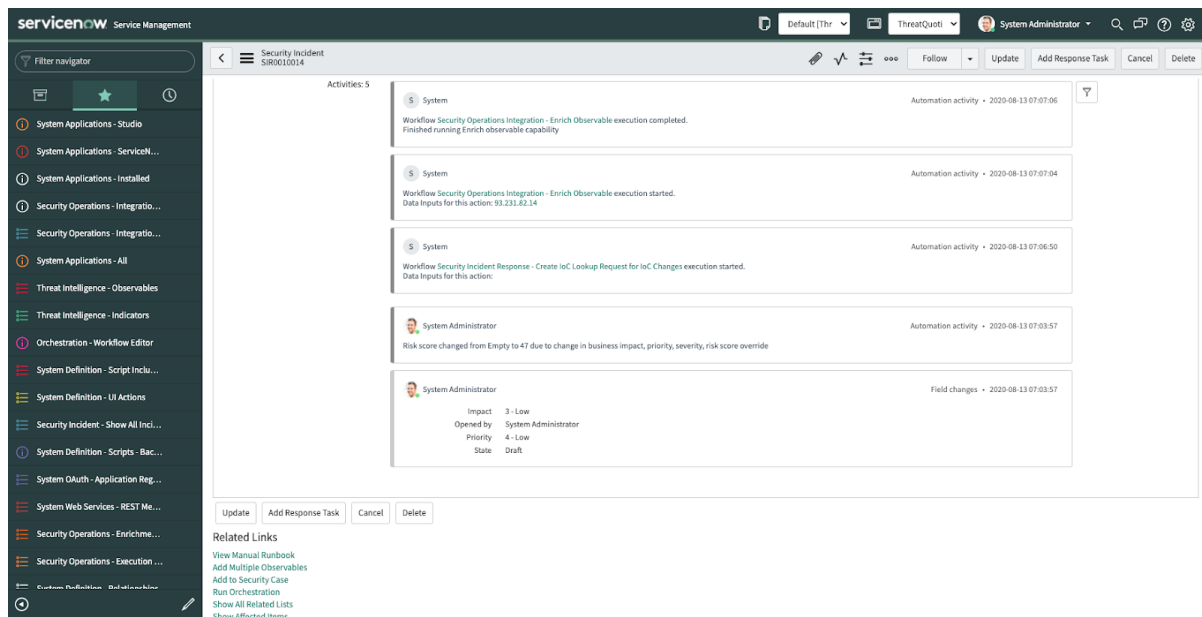
## 3. Add observables to the Security Incident.

The screenshot shows the ServiceNow Security Incident form with the 'Configuration Items' tab selected. The 'Related Links' section includes links for 'View Manual Runbook', 'Add Multiple Observables', 'Add to Security Case', 'Run Orchestration', 'Show All Related Lists', 'Show Affected Items', 'Show Related Items', 'Show iOC', 'Show Enrichment Data', and 'Show Response Tasks'. The 'Configuration Items' table is empty, displaying 'No records to display'. The table headers include Configuration Item, Class, Support group, Owned by, Applied, Applied date, Manual proposed change, and Updated.



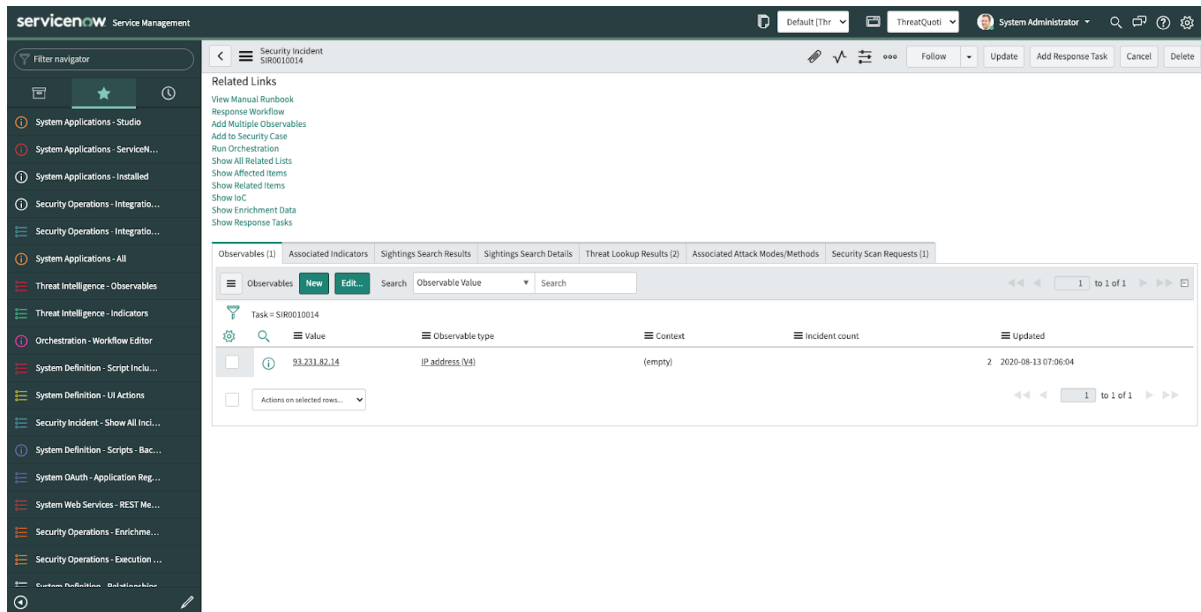
4. Click on Submit and wait for automatic threat lookup activity to complete.

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 interface for a Security Incident (SIR0010014). The left sidebar contains a Filter navigator with various system applications and security operations links. The main content area displays the 'Threat Lookup Results (2)' tab, which shows a table of observables. The table has columns for Value, Observable type, Context, Incident count, and Updated. One observable is listed with the value '93.231.82.14' and type 'IP.address (V4)'. The incident count is 2, and the updated date is 2020-08-13 07:06:04. The top of the page shows the ServiceNow logo, the incident ID, and the user 'System Administrator'.

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 Threat Lookup interface. The left sidebar contains a filter navigator with various system applications and security operations categories. The main content area displays a table of threat lookup results. The table has columns for Observable, Integration vendor, Finding, Result value, Details, Source Engine, Engine version, and Retrieval date. Two results are visible, both for the observable 93.231.82.14, with integration vendor ThreatQuotient and finding Unknown. The result value for both is 'Observable was found in ThreatQ'.

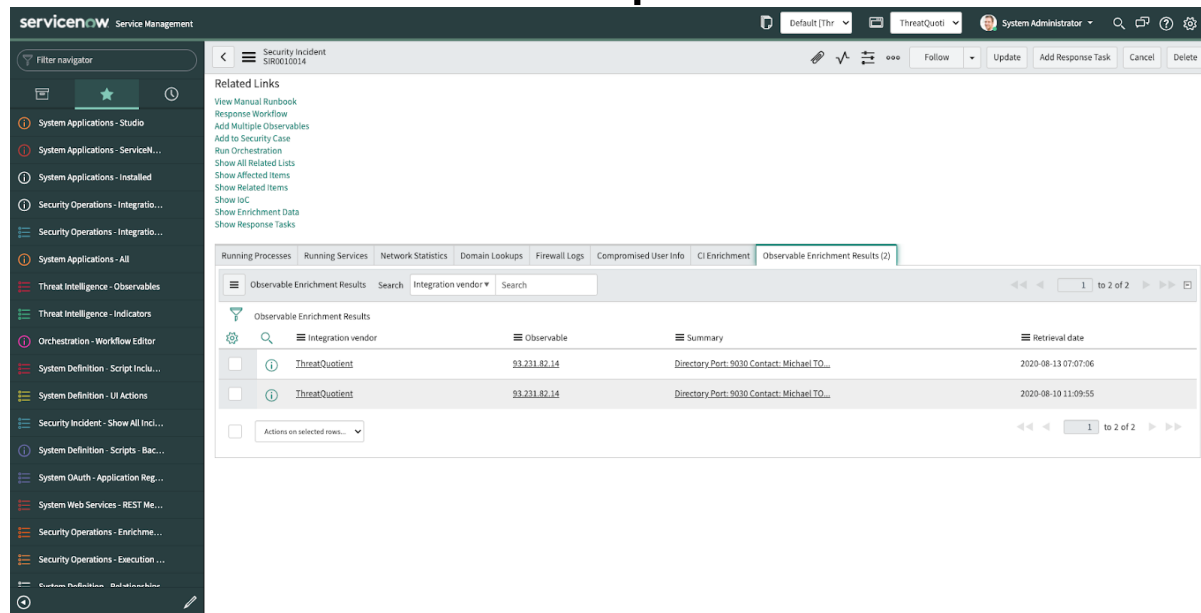
## Viewing Observable Enrichment Results

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

The screenshot shows the ServiceNow Threat Lookup interface with the details of an observable enrichment result for the observable 93.231.82.14. The details are displayed in a form with the following fields:

- Observable: 93.231.82.14
- Integration vendor: ThreatQuotient
- Finding: Unknown
- Source Engine: ThreatQ
- First found: 2020-08-09 11:39:45
- Engine version: 4.39.0-850
- Security tags:
- Retrieval date: 2020-08-13 07:07:05
- 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: A JSON object containing detailed information about the observable, including its status, creation date, last updated date, and sources.

# Enrichment Details Example



The screenshot shows the ServiceNow interface for a Security Incident (SRI0010014). The left sidebar contains a filter navigator with various system applications and security operations categories. The main content area displays the incident details and a list of related links. Below the links, there are tabs for different enrichment views: Running Processes, Running Services, Network Statistics, Domain Lookups, Firewall Logs, Compromised User Info, CI Enrichment, and Observable Enrichment Results (2). The 'Observable Enrichment Results' tab is selected, showing a table of enrichment results. The table has columns for Integration vendor, Observable, Summary, and Retrieval date. Two rows are visible, both for ThreatQuotient with the observable 93.231.82.14. The first row shows a directory port 9030 contact for Michael TO... retrieved on 2020-08-13 07:07:06. The second row shows a directory port 9030 contact for Michael TO... retrieved on 2020-08-10 11:09:55. Below the table, there is a dropdown menu for 'Actions on selected rows...' and a pagination bar showing 1 to 2 of 2 results.

ServiceNow Service Management

Default [Thr] ThreatQuot System Administrator

Filter navigator

Security Incident SRI0010014

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 Search

Integration vendor	Observable	Summary	Retrieval date
ThreatQuotient	93.231.82.14	Directory Port: 9030 Contact: Michael TO...	2020-08-13 07:07:06
ThreatQuotient	93.231.82.14	Directory Port: 9030 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 1.1.0**
  - Added new Oauth configuration option, **TQ Attributes Location**, that lets you specify the table where indicator attributes are saved.
  - Validated app for San Diego and Tokyo.
- **Version 1.0.9**
  - Initial release