

ThreatQuotient



ServiceNow App User Guide

Version 1.2.0

August 01, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

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
Permissions and Roles	7
ServiceNow Required Plugins	8
OAuth Client ID and Client Secret.....	9
Installation.....	10
Configuration	11
Usage.....	14
Creating a Security Incident	14
ThreatQ Lookup	17
Manual Threat Lookup	17
Auto Threat Lookup	21
Observable Enrichment	26
Manual Observable Enrichment.....	26
Auto Observable Enrichment	30
Troubleshooting	35
Increase Field of Input Field	35
Application Logs	35
Upgrading Application	36
Known Issues / Limitations	37
Change Log	38

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 App Version	1.2.0
Compatible with ThreatQ Versions	>=5.16.0
Validated	San Diego, Tokyo, Utah
Support Tier	ThreatQ Supported

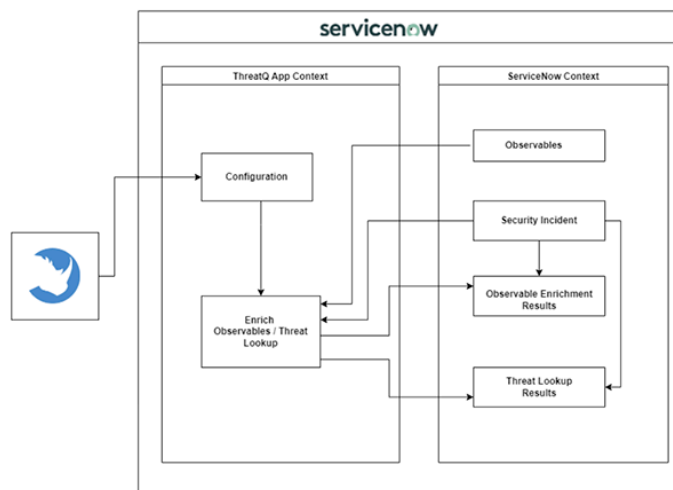
Introduction

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 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

Review the following requirements before attempting to install the app.

Permissions and Roles

The following ServiceNow role and the permissions that are required to install the application and to use it to view and manage the vulnerability integration on ServiceNow.

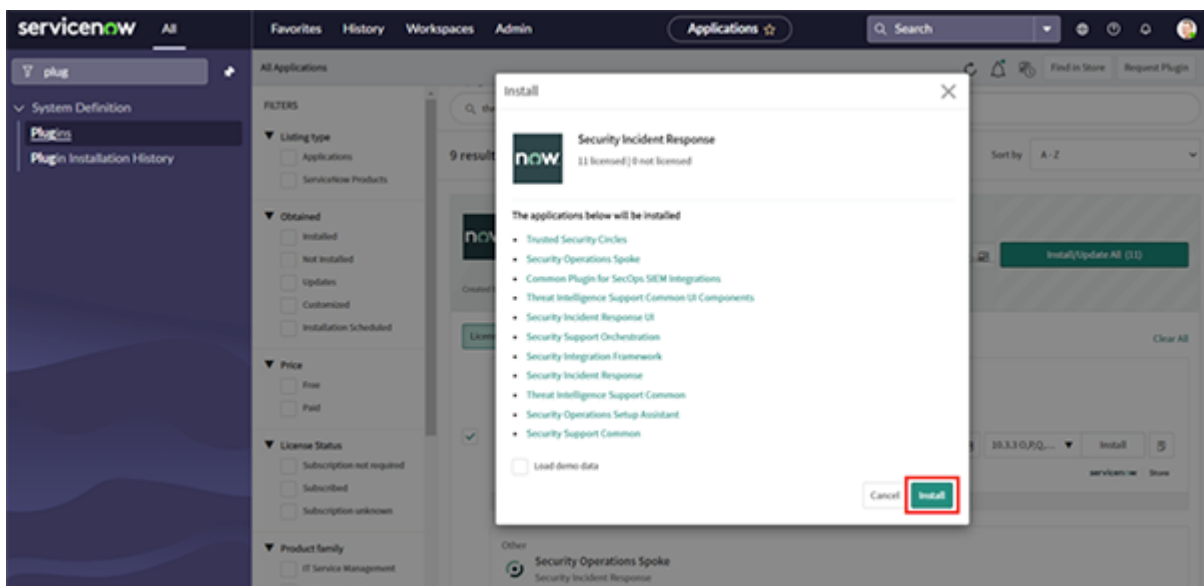
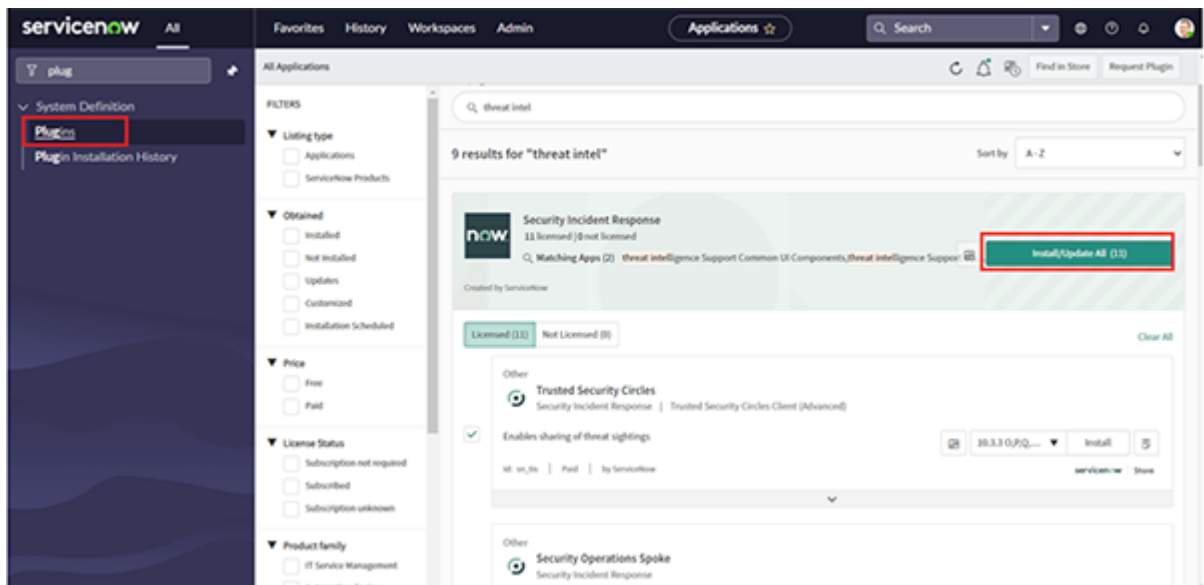
ROLE	PERMISSIONS
System Administrator (admin)	<ul style="list-style-type: none">• Installation of the application• Configure integration tile• Perform Observable Enrichment and Threat Lookup• See ThreatQ details in Threat Lookup and Observable Enrichment Results• Uninstallation of the application

ServiceNow Required Plugins

The Threat Intelligence and Security Incident Response ServiceNow plugins are required by app and must be installed and activated.

To install this plugins:

1. Log into your instance with your user credentials.
2. Verify you have the system administrator (admin) role.
3. Navigate to **System Definition** -> **Plugins** in your instance.
4. Locate and still both plugins, **Threat Intelligence** and **Security Incident Response**, using the search.



OAuth Client ID and Client Secret

The ServiceNow App requires you to enter your **OAuth Client ID** and **OAuth Client Secret** when [configuring](#) the app. 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:

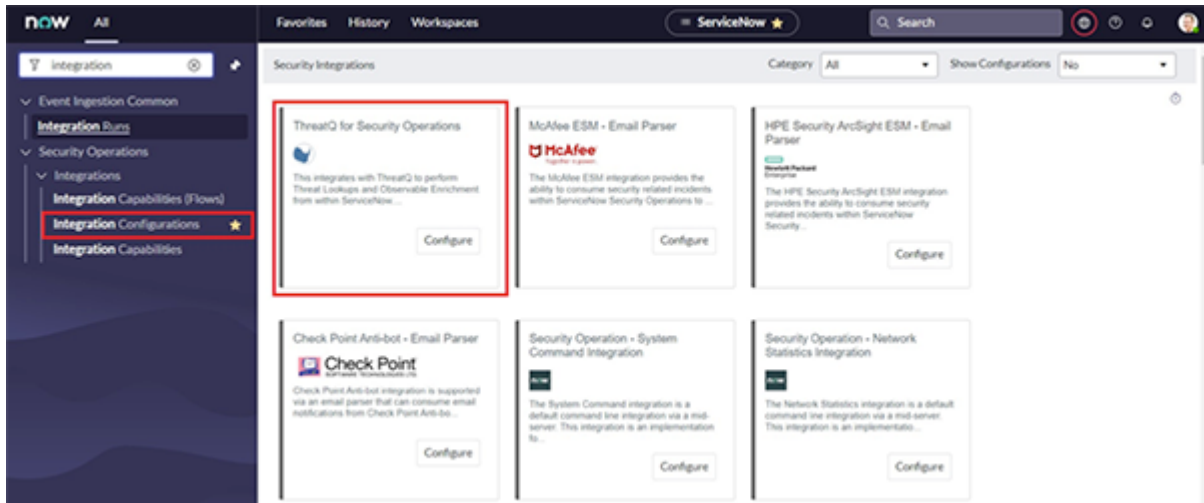
1. Use the Filter navigator and navigate to **System Applications - ServiceNow Store**.
2. Search for **ThreatQ** within the Store Application and then click the **Install** button.



Configuration


Within the ServiceNow interface:

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



2. Complete the following configuration fields:

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.
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.
Attributes	Specify comma separated ThreatQ attributes names which need to be fetched for indicator.

FIELD	DESCRIPTION
<div>  <p>To get a list of the attributes in ThreatQ, navigate to Settings -> Object Management -> Attribute Management.</p> </div>	
Object Properties	<p>Specify comma separated ThreatQ properties names which need to be fetched for indicator. The property names for the enriched indicator are: Type, Status, Score, Sources, Tags.</p> <p>Additionally, relationships can also be ingested from ThreatQ by specifying their names: Adversaries, Asset, Attack Pattern, Campaign, Course of Action, Exploit Target, Events, Identity, Incident, Intrusion Set, Malware, Signatures, Type, TTP, Tool, Vulnerability</p>
TQ Attribute Location	<p>Specify the table where you want to save each indicator's attributes. Options include either Threat Lookup Results or Observable Enrichment Results.</p>

ThreatQ for Security Operations Configuration




* ThreatQ Hostname/IP	<input type="text" value="https://abc.threatq.com/"/>
* OAuth Client ID	<input type="text" value="OAuth Client ID"/>
* OAuth Client Secret	<input type="password" value="*****"/>
* Malicious Finding Threshold	<input type="text" value="7"/>
* Attributes	<input type="text" value="None"/>
* Object Properties	<input type="text" value="Type, Status, Score, Sources, Tags"/>
* TQ Attributes Location	<input type="text" value="Observable Enrichment Results"/>

Cancel

Submit

3. Click on **Submit**.

ThreatQ for Security Operations Configuration
×



* ThreatQ
Hostname/IP

* OAuth Client ID

* OAuth Client
Secret

* Malicious Finding
Threshold

* Attributes

* Object Properties

* TQ Attributes
Location

Cancel

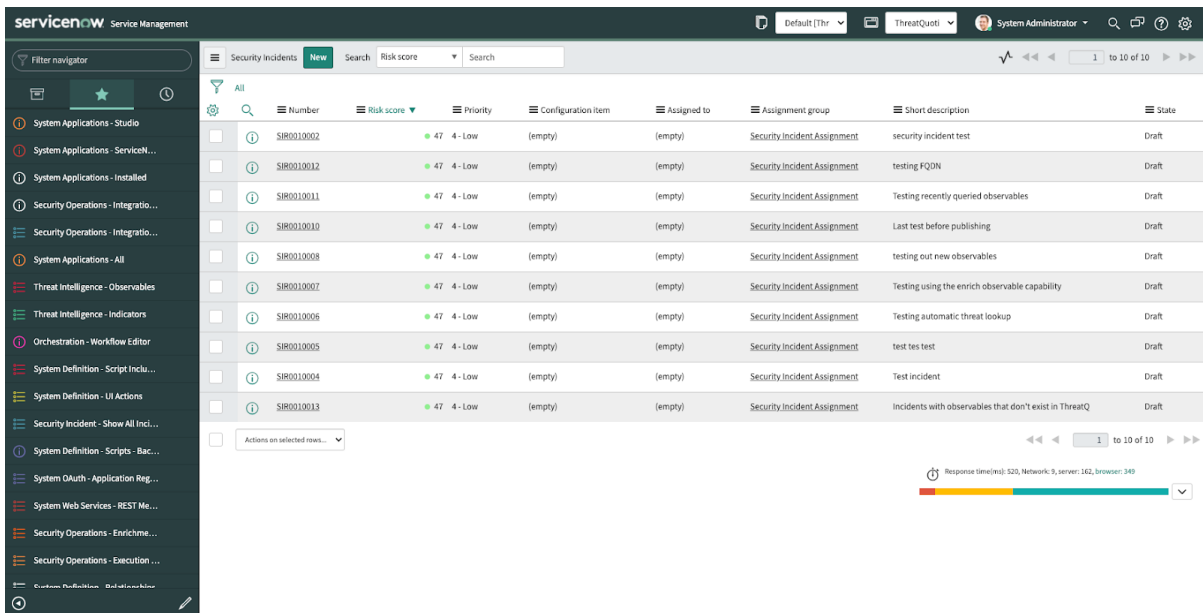
Submit

Usage

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

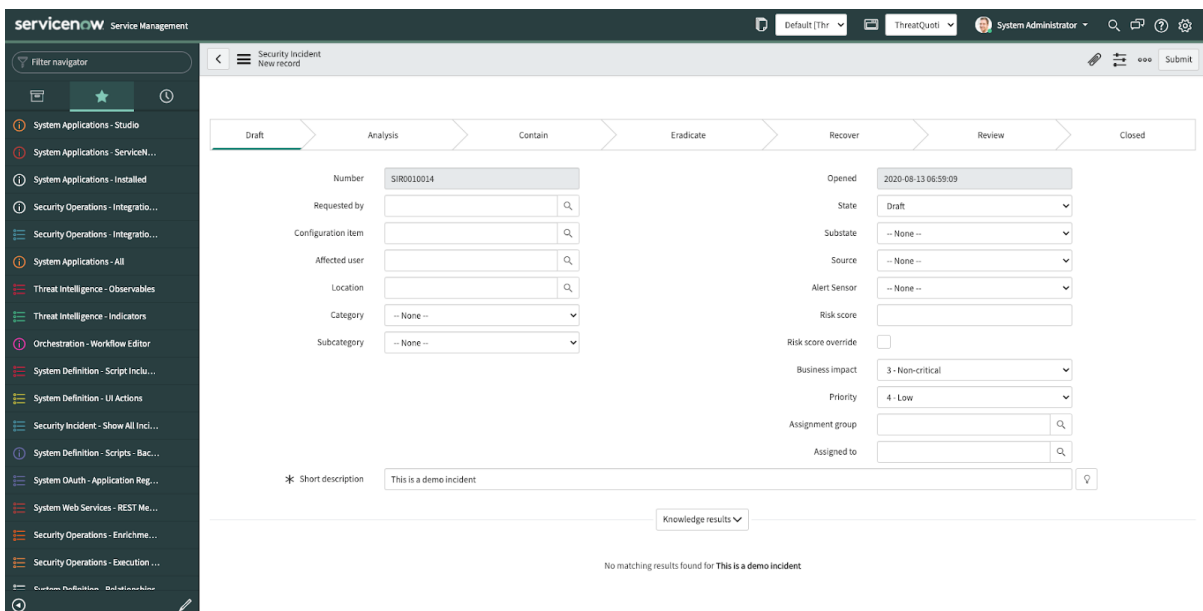
Creating a Security Incident

1. Create a new Security Incident.



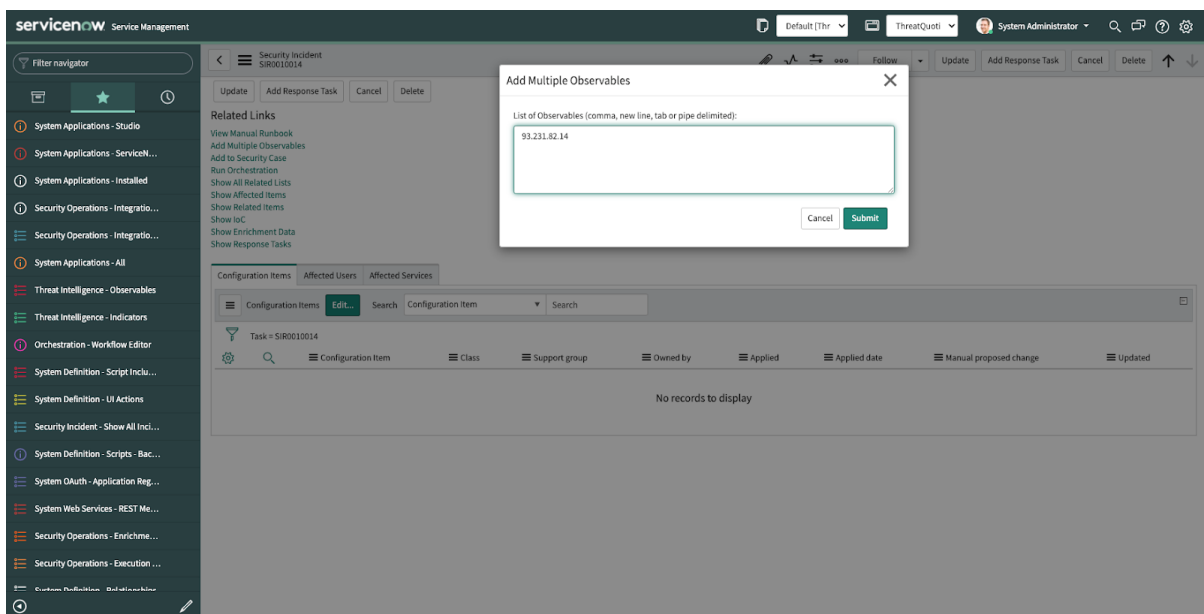
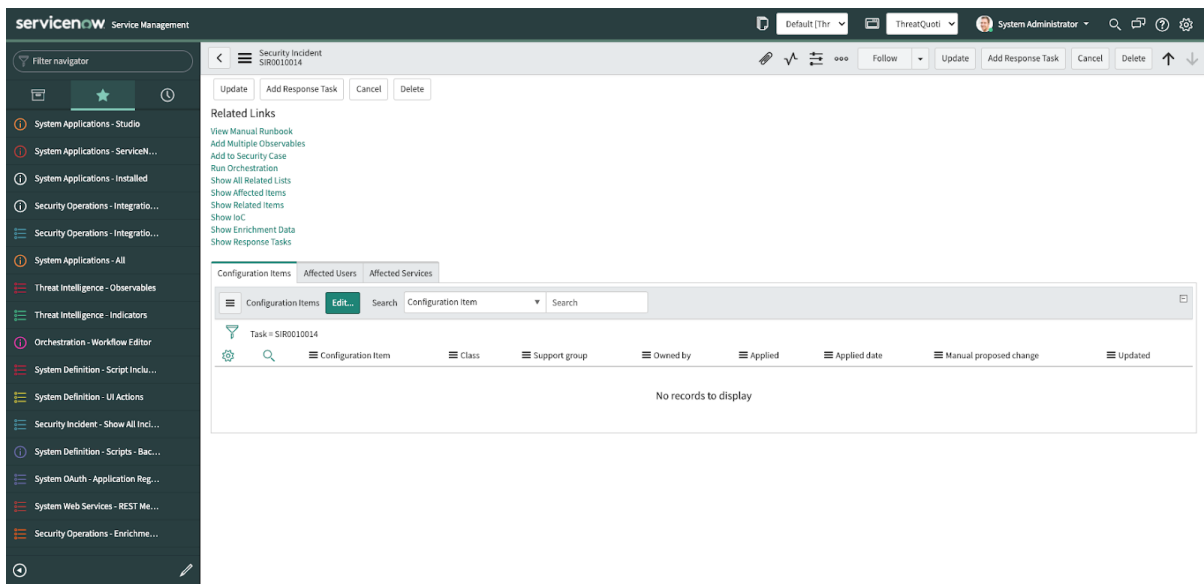
The screenshot shows the ServiceNow Security Incidents list view. The left sidebar contains a filter navigator with various system applications and security operations categories. The main table lists security incidents with columns for Number, Risk score, Priority, Configuration item, Assigned to, Assignment group, Short description, and State. The incidents are all in 'Draft' state and have a risk score of 47 and priority of 4 - Low. The 'Short description' column contains various test scenarios like 'security incident test', 'testing FQDN', 'Testing recently queried observables', etc. At the bottom right, there is a response time indicator showing 349ms.

2. Give the Security Incident a short description.



The screenshot shows the ServiceNow Security Incident form view for a new record. The form is in 'Draft' state and shows various fields for incident details. The 'Number' field is populated with 'SIR0010014'. The 'Opened' date is '2020-08-13 06:59:09'. The 'State' is 'Draft'. The 'Short description' field contains the text 'This is a demo incident'. The 'Knowledge results' section at the bottom shows 'No matching results found for This is a demo incident'.

3. Add observables to the Security Incident.



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

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

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 Incl...

System Definition - Scripts - Bac...

System OAuth - Application Reg...

System Web Services - REST Me...

Security Operations - Enrichme...

Security Operations - Execution ...

Enrichment Profiles - Build and Manage

Security Incident

SIR0010014

Follow

Update

Add Response Task

Cancel

Delete

Activities: 5

System

Workflow Security Operations Integration - Enrich Observable execution completed. Finished running Enrich observable capability

Automation activity • 2020-08-13 07:07:06

System

Workflow Security Operations Integration - Enrich Observable execution started. Data Inputs for this action: 93.223.82.34

Automation activity • 2020-08-13 07:07:04

System

Workflow Security Incident Response - Create IoC Lookup Request for IoC Changes execution started. Data Inputs for this action:

Automation activity • 2020-08-13 07:06:50

System Administrator

Risk score changed from Empty to 47 due to change in business impact, priority, severity, risk score override

Automation activity • 2020-08-13 07:03:57

System Administrator

Field changes

2020-08-13 07:03:57

Impact

3 - Low

Opened by

System Administrator

Priority

4 - Low

State

Draft

Update

Add Response Task

Cancel

Delete

Related Links

View Manual Runbook

Add Multiple Observables

Add to Security Case

Run Orchestration

Show All Related Links

Show Affected Items

ServiceNow App User Guide
Version 1.2.0

16

ThreatQ Lookup

The steps below are for performing manual and auto Threat Lookups.

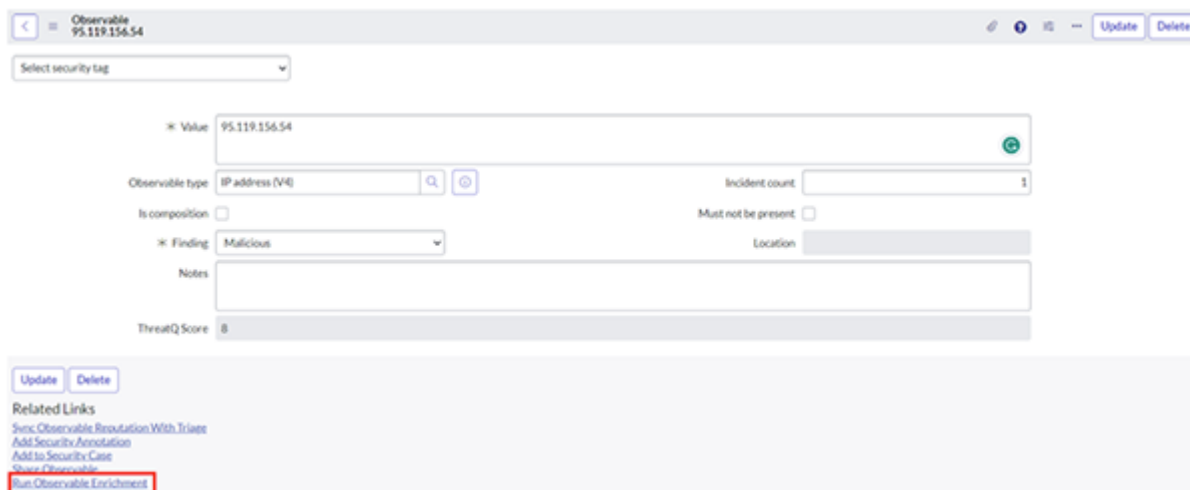
Manual Threat Lookup

The Threat lookup is performed to find if any observable is malicious or not.

SETTING	DETAILS
Role Required	admin
Prerequisites	Set Threat Lookup Results as the input in the TQ Attribute Location.

Performing a Manual Threat Lookup:

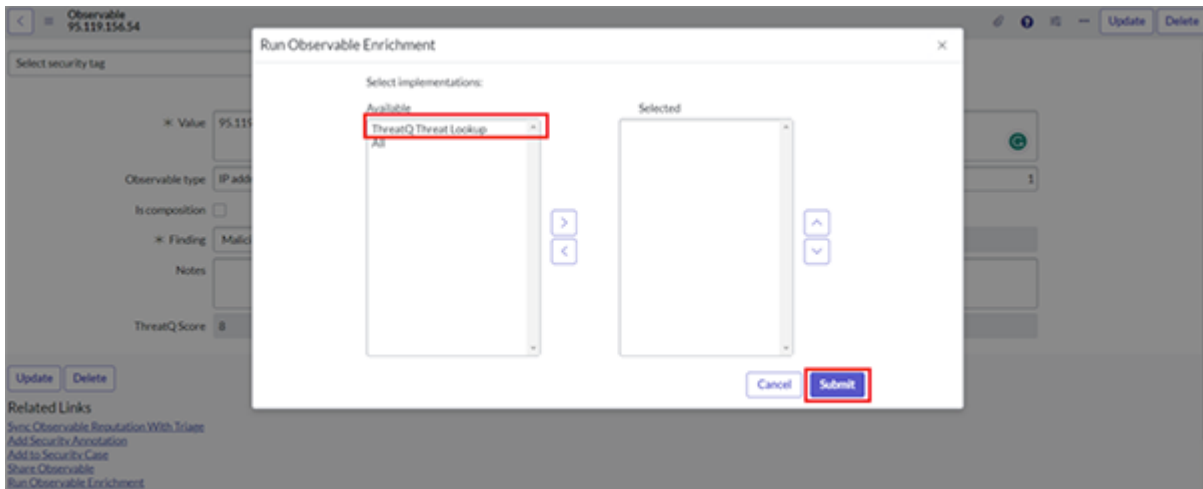
1. Navigate to **Threat Intelligence > Observables**.
2. Click on any observable of type **IP**, **URL** or **Hash** and then click on the **Run Observable Enrichment** option under the *Related Links* heading.



The screenshot shows the ThreatQ Observable interface for the observable 95.119.156.54. The interface includes a search bar, a dropdown for 'Select security tag', and a form for 'Value' (95.119.156.54). Below the value field, there are fields for 'Observable type' (IP address (V4)), 'Incident count' (1), 'Is composition' (checkbox), 'Must not be present' (checkbox), 'Finding' (Malicious), and 'Location'. A 'Notes' field and a 'ThreatQ Score' (8) are also visible. At the bottom, there is a 'Related Links' section with several links, including 'Run Observable Enrichment', which is highlighted with a red box.

A pop-up window will open.

3. Select **ThreatQ Threat Lookup** and click on **Submit**.

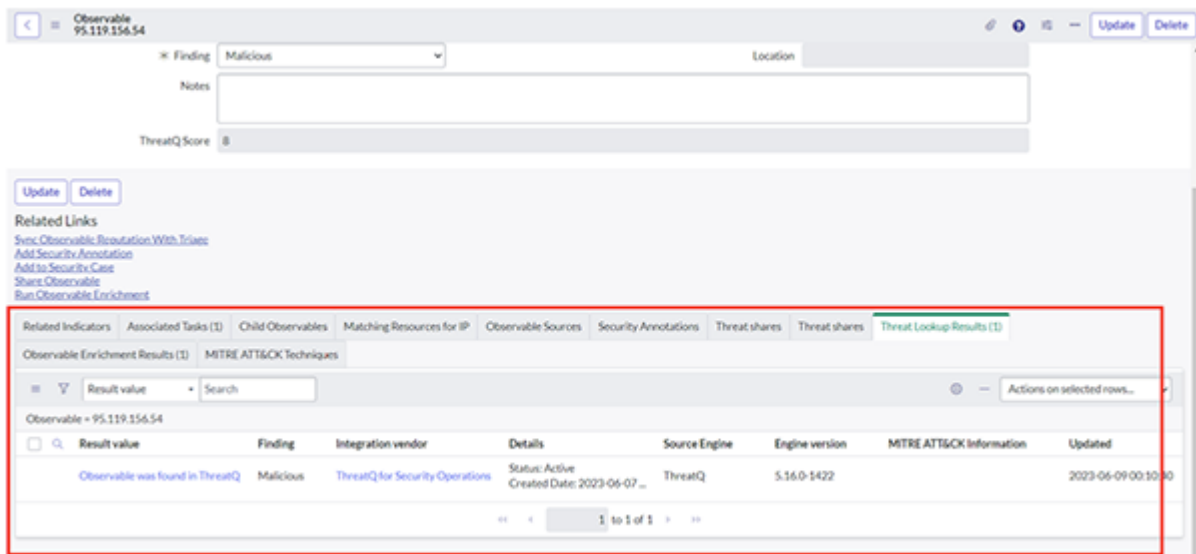



4. The lookup will start and you will see lookup results, once the process is complete, under the *Threat Lookup Results* section.



Threat lookup on the same observable from ThreatQ will be performed once in 24 hours only.

5. To view the **Threat Lookup Results**, open the Observable and scroll down to see the **Threat Lookup Results** record created for the observable.



6. Open the **Threat Lookup Results** record to view the details of lookup.
7. From the top left, click on the  icon > **View** > **ThreatQ** to view the details of the observable.

Threat Lookup Result 95.119.156.54 View ThreatQ		
Testing: -ip="created_at":"2023-06-06 05:42:18";updated_at":"2023-06-06 05:42:18";touched_at":"2023-06-13 09:25:23";object_id":"13";object_code":"asset";object_name":"Assets";object_name_plural":"Assets";pivot":{"id":"34203";created_at":"2023-06-06 06:45:54";updated_at":"2023-06-06 06:45:54";course_of_action":{"id":"248";value":{"action_1":{"status_at":{"multi_type_at":{"multi_created_at":"2023-06-02 10:26:59";updated_at":"2023-06-02	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	
ThreatQ Attributes	uptime: 3569 version: Tor 0.4.7.13	
ThreatQ Sources	www.eutanuma.uk Tor Node List, Cnort	
ThreatQ Tags	Test tag1, Test tag2, demo1	
ThreatQ Adversaries	admin@336, Ajax Security Team, AjaxTM	
ThreatQ Asset	asset_1, asset_2, Asset0-1	
ThreatQ Attack Pattern	Attack pattern 2, Attack Pattern-1	
ThreatQ Campaign	C0011, C0018	
ThreatQ Course Of Action	action_1, action_2, action_3	
ThreatQ Events	SECC0001011 - ANZ Test, SECC0001012 - Adversary Cricket1 has gained access to the grain silos, SECC0001014 - dev app	
ThreatQ Exploit Target	Exploit Target1, Exploit Target-1	



ThreatQ Comments will not be populated in worknotes if enrichment is executed from an observable table.

To avoid duplicity, the value of `created_at` is ingested in the First Found field of the Threat Lookup Result table.

Auto Threat Lookup

Auto Threat Lookup can be performed on an observable by attaching to a security incident.

SETTING

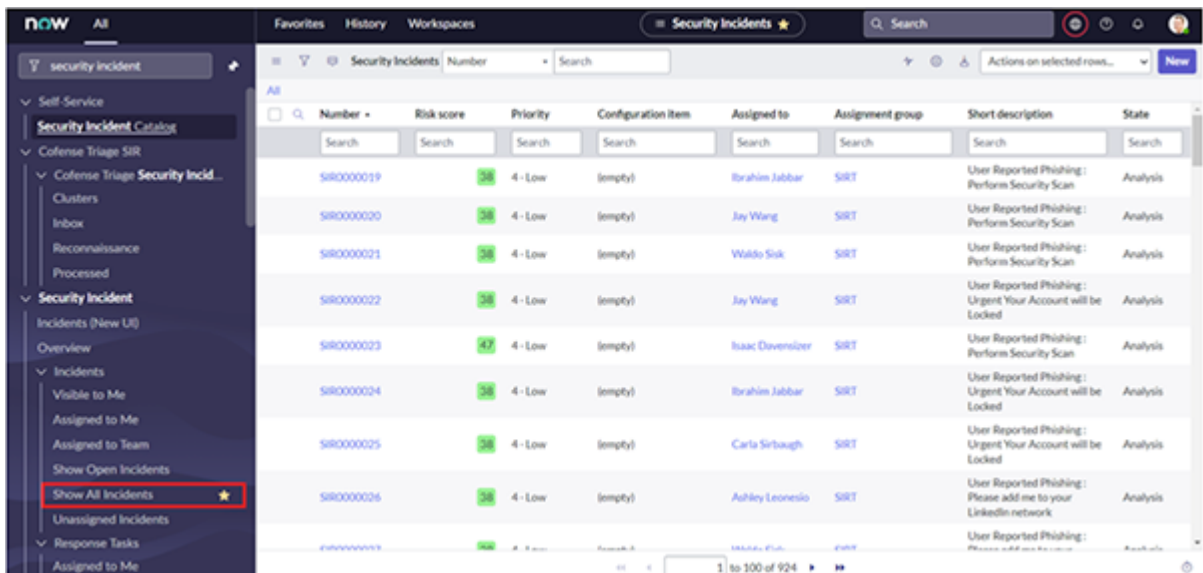
Role Required admin

DETAILS

Prerequisites Set **Threat Lookup Results** as the input in the **TQ Attribute Location**.

Performing Auto Threat Lookup:

1. Navigate to **Security Incident > Incidents > Show All Incidents**.



Number	Risk score	Priority	Configuration item	Assigned to	Assignment group	Short description	State
SIR0000019	28	4 - Low	(empty)	Ibrahim Jabbar	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000020	28	4 - Low	(empty)	Jay Wang	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000021	28	4 - Low	(empty)	Waldo Sisk	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000022	28	4 - Low	(empty)	Jay Wang	SIRT	User Reported Phishing: Urgent Your Account will be Locked	Analysis
SIR0000023	47	4 - Low	(empty)	Isaac Doversizer	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000024	28	4 - Low	(empty)	Ibrahim Jabbar	SIRT	User Reported Phishing: Urgent Your Account will be Locked	Analysis
SIR0000025	28	4 - Low	(empty)	Carla Sirbaugh	SIRT	User Reported Phishing: Urgent Your Account will be Locked	Analysis
SIR0000026	28	4 - Low	(empty)	Ashley Leonasio	SIRT	User Reported Phishing: Please add me to your LinkedIn network	Analysis

2. Click on the security incident that the observable is linked to and then click on **Show IOC** under the *Related Links* section.

- Click **New**, located under the *Associated Observables* section, to create a new observable. Link the observable to the security incident or click **Edit** to add links an existing observable.

Once the observable is linked to the incident, auto threat lookup is started.



Worknotes will be generated in the **Incident Details** tab.

Threat Lookup Results can also be accessed via the **ThreatQ Enrichment** tab.

Security Incident
SIR0000020


Update Add Response Task Cancel Delete

Knowledge results >

Incident Details Related Records MITRE ATT&CK Card Test ThreatQ Enrichment

Threat Lookup Results 1 to 15 of 15

	Observable	Integration vendor	Finding	Result value	Details	Source Engine	Engine version
X	95.119.116.54	ThreatIQ for Security Operations	Malicious	Observable was found in ThreatIQ	Status: Active Created Date: 2023-06-07 ...	ThreatIQ	5.16.0.14C
X	8.16.0.42	VirusTotal - VT	Unknown		The IP 8.16.0.42 has not been detected b...	VirusTotal API	v2
X	127.0.0.1	ThreatCrowd	Malicious	Most users have voted this malicious	This observable has a user vote weight o...	ThreatCrowd API	v2
X	127.0.0.1	VirusTotal - VT	Malicious	100 engine(s) reported the observable as...	http://cid/bazediapreaglad.to/- 3 of 71...	VirusTotal API	v2
X	8.16.0.42	VirusTotal - VT	Unknown		The IP 8.16.0.42 has not been detected b...	VirusTotal API	v2
X	127.0.0.1	ThreatCrowd	Malicious	Most users have voted this malicious	This observable has a user vote weight o...	ThreatCrowd API	v2
X	A82B794C9894A4FDB9EDAA8A04C318BA89723DA6...	VirusTotal - VT	Unknown		Hash value not found in VirusTotal.	VirusTotal API	v2
X	127.0.0.1	VirusTotal - VT	Malicious	100 engine(s) reported the observable as...	http://cid/bazediapreaglad.to/- 3 of 71...	VirusTotal API	v2
X	67.231.157.3	VirusTotal - VT	Unknown		The IP 67.231.157.3 has not been detecte...	VirusTotal API	v2
X	127.0.0.1	VirusTotal - VT	Malicious	100 engine(s) reported the observable as...	http://cid/bazediapreaglad.to/- 3 of 71...	VirusTotal API	v2
X	8.16.0.36	VirusTotal - VT	Unknown		The IP 8.16.0.36 has not been detected b...	VirusTotal API	v2
X	127.0.0.1	ThreatCrowd	Malicious	Most users have voted this malicious	This observable has a user vote weight o...	ThreatCrowd API	v2
X	209.85.166.68	ThreatCrowd	Unknown	An equal number of users have voted this...	This observable has a user vote weight of 0	ThreatCrowd API	v2
X	8.16.0.42	VirusTotal - VT	Unknown		The IP 8.16.0.42 has not been detected b...	VirusTotal API	v2

- Open the threat lookup result and click on the  icon, located to the top left, and select **View > ThreatQ** to view the details of the observable.

Threat Lookup Result 95.119.156.54 View ThreatQ	
Observable	95.119.156.54
Integration vendor	ThreatQ for Security Operations
Finding	Malicious
First found	2023-06-07 09:01:19
ThreatQ score	8
ThreatQ status	Active
External link	https://services.threatq.com/indicators/277636/details
Result value	Observable was found in ThreatQ
Details	Status: Active Created Date: 2023-06-07 16:05:19 Last Updated Date: 2023-06-08 06:42:44 Sources: www.danume.uk Tor Node List, Crest Score: 8 Optimal: 3569 version: Tor 0.4.7.13 Malware: Machete, MacSpys, Mafabits Adversaries: adm3g338, Ajax Security Team, AjaxTM
Raw data	<pre>misp.attack.mitre.org/groups/users is security researchers assess the ip:attack.misp.attack.mitre.org/software's user name may be inspired by an argentinian cartoon character that has been popular as a means of political commentary since the 1960s. ICitation: Sentinel Labs Malware Sept 2020:13 16:11:03"/object_id":"Malware/object_name":"Malware/object_name_plural":"Malware/plural"/"IP:34225"/created_at":"2021-09-22 05:58:26"/updated_at":"2021-09-22 05:58:26"/touched_at":"2021-09-22 05:58:26"/adversary":{"id":"174"/name":"adming338"/created_at":"2021-09-22 05:58:26"/updated_at":"2021-09-22 05:58:26"/touched_at":"2021-09-22 05:58:26"}ip":{"id":"34198"/name":"adming338"/created_at":"2021-09-22 05:58:26"/updated_at":"2021-09-22 05:58:26"/touched_at":"2021-09-22 05:58:26"}team":{"id":"34199"/name":"Ajax Security Team"/created_at":"2021-09-22 05:58:26"/updated_at":"2021-09-22 05:58:26"/touched_at":"2021-09-22 05:58:26"}ip":{"id":"34199"/name":"Ajax Security Team"/created_at":"2021-09-22 05:58:26"/updated_at":"2021-09-22 05:58:26"/touched_at":"2021-09-22 05:58:26"}ip":{"id":"34200"/name":"AjaxTM"/created_at":"2021-09-22 05:58:26"/updated_at":"2021-09-22 05:58:26"/touched_at":"2021-09-22 05:58:26"}tag":{"id":"13"/name":"Test tag1"/created_at":"2021-06-08 06:42:13"/updated_at":"2021-06-08 06:42:13"/touched_at":"2021-06-08 06:42:13"}tag":{"id":"14"/name":"Test tag2"/created_at":"2021-06-08 06:42:13"/updated_at":"2021-06-08 06:42:13"/touched_at":"2021-06-08 06:42:13"}tag":{"id":"15"/name":"Test tag3"/created_at":"2021-06-08 06:42:13"/updated_at":"2021-06-08 06:42:13"/touched_at":"2021-06-08 06:42:13"}comment":{"creator_source_ip":"32"/created_at":"2023-06-08 06:42:57"/updated_at":"2023-06-08 06:42:57"/"id":"50"/indicator_ip:"277636"/value":"/Test comment1"/></pre>

ThreatQ Attributes	uptime: 3549 version: Tor 0.4.7.13
ThreatQ Sources	www.usdenuk Tor Node List, Crest
ThreatQ Tags	Test tag1, Test tag2, demo1
ThreatQ Adversaries	admin@335, Ajax Security Team, AjaxTM
ThreatQ Asset	asset 1, asset 2, Asset - 1
ThreatQ Attack Pattern	Attack pattern 2, Attack Pattern-1
ThreatQ Campaign	C0011, C0018
ThreatQ Course Of Action	action 1, action 2, action 3
ThreatQ Events	SECC0001011 - ANZ Test, SECC0001012 - Adversary Cricket1 has gained access to the grain silos, SECC0001014 - dev app
ThreatQ Exploit Target	Exploit Target1, Exploit Target - 1

ThreatQ Identities	Identity-1
ThreatQ Incident	Incident1, Incident - 1
ThreatQ Intrusion Set	Intrusion Set1, Intrusion set- 1
ThreatQ Malware	Machete, MacSpy, Mafalda
ThreatQ Signatures	Test SignatureTest Signature
ThreatQ Tools	TaskBot, Tool - 1, Tor
ThreatQ TTP	Http1, TTP-1
ThreatQ Vulnerability	Vulnerability1, Vulnerability - 1

ThreatQ Description: Added Description For Testing.



If there are any ThreatQ comments for the observable then worknotes will be updated with ThreatQ comments.

Activities: 250	System Workflow Security Operations Integration - Enrich Observable execution completed. Finished running enrich observable capability	Automation activity • 2023-06-14 00:22:08 4m ago
	System [ThreatQ] Comments for observable "95.119.156.54": Test comment1, Test comment2	Work notes • 2023-06-14 00:22:07 4m ago
	System Workflow Security Operations Integration - Enrich Observable execution started. Data inputs for this action: 95.119.156.54	Automation activity • 2023-06-14 00:22:00 4m ago

To avoid duplicity, the value of created_at is ingested in the First Found field of the Threat Lookup Result table.

Observable Enrichment

The following steps will be performing manual and auto observable enrichment.

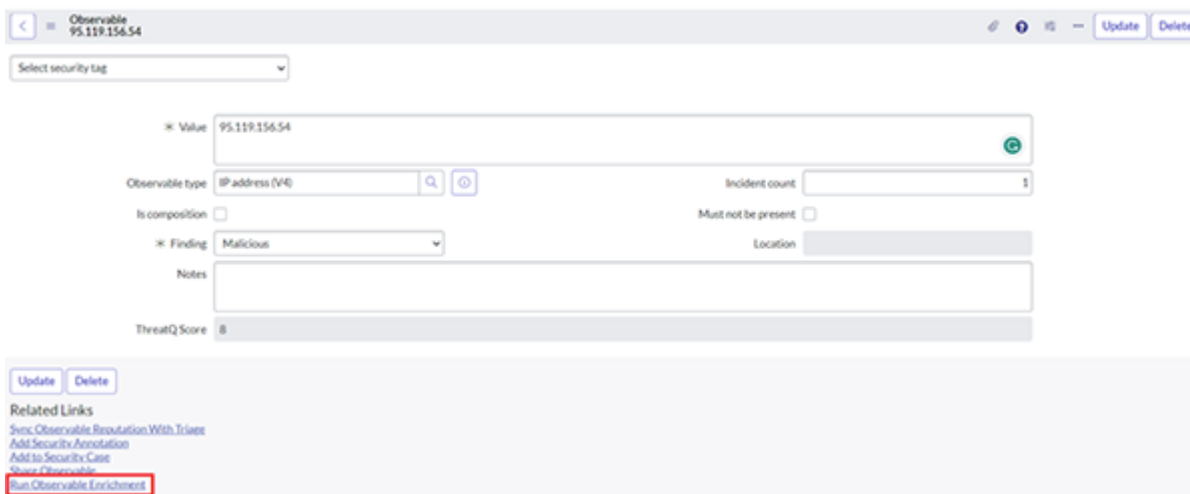
Manual Observable Enrichment

The Observable Enrichment is performed to fetch additional information related to the observable.

SETTING	DETAILS
Role Required	admin
Prerequisites	Set Observable Enrichment Results as the input in the TQ Attribute Location .

Performing Manual Observable Enrichment:

1. Navigate to **Threat Intelligence > Observables**.
2. Click on any observable of type **IP**, **URL** or **Hash** and then click on the **Run Observable Enrichment** option under the *Related Links* heading.



Observable: 95.119.156.54

Select security tag

* Value: 95.119.156.54

Observable type: IP address (V4)

Incident count: 1

Is composition: ☐

* Finding: Malicious

Must not be present: ☐

Location:

Notes:

ThreatQ Score: B

Update Delete

Related Links

- [Sync Observable Resolution With Triage](#)
- [Add Security Annotation](#)
- [Add to Security Case](#)
- [View Observable](#)
- [Run Observable Enrichment](#)**

A pop-up window will open.

3. Select **ThreatQ Threat Lookup** and click on **Submit**.

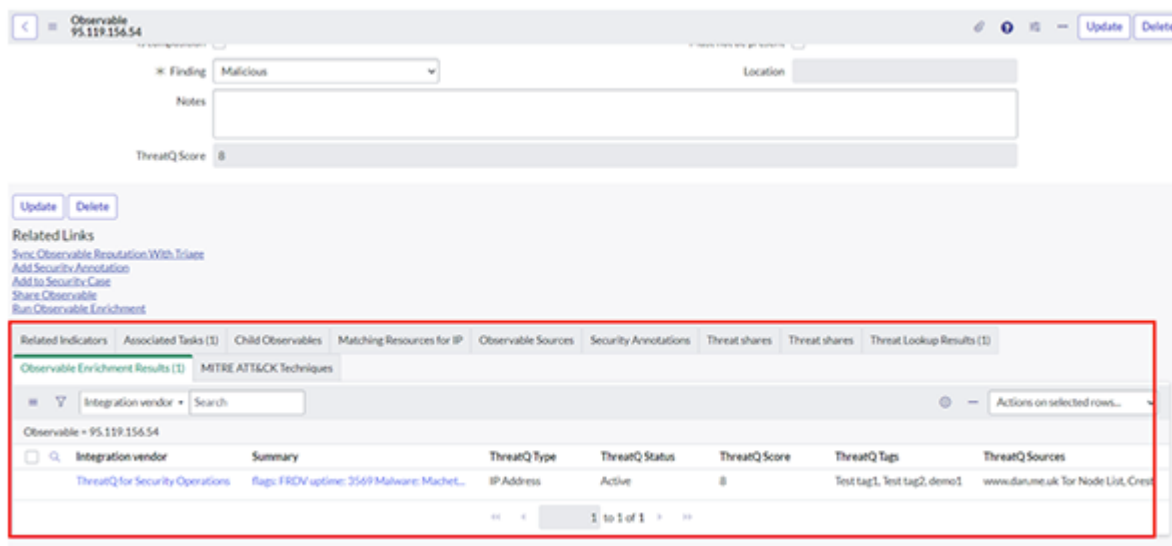


4. The enrichment will start and you will see lookup results, once the process is complete, under the *Observable Enrichment Results* section.



Observable enrichment on the same observable from Threat will be performed once in 24 hours only. Threat Lookup would also get performed for the observable even if **Observable Enrichment Results** is the provided input in **TQ Attribute Locations**.

5. To view the **Observable Enrichment Results**, open the **Observable** and scroll down to locate the **Observable Enrichment Results** record created for the observable.



6. Open the **Observable Enrichment Results** record to view the details of the lookup.
7. From the top left, click on the **hamburger icon** > **View** > **ThreatQ** to view the details of the observable.

Observable Enrichment Result	
95.119.134.54 View ThreatQ	
ThreatQ Attributes	<pre>{ "created_at": "2023-06-07 11:19:59", "hostname": "testhost" }</pre>
ThreatQ Sources	www.eudaturne.uk Tor Node List, Crest
ThreatQ Tags	Test tag1, Test tag2, demo1
ThreatQ Adversaries	adming338, Ajax Security Team, AjaxTM
ThreatQ Asset	asset 1, asset 2, Asset0-1
ThreatQ Attack Pattern	Attack pattern 2, Attack Pattern-1
ThreatQ Campaign	C0011, C0018
ThreatQ Course Of Action	action 1, action 2, action 3
ThreatQ Events	SECC00001011 - ANZ Test, SECC00001012 - Adversary Cricket1 has gained access to the grain silos, SECC00001014 - dev app
ThreatQ Exploit Target	Exploit Target1, Exploit Target-1

Observable Enrichment Result
95.119.154.54 View ThreatQ

ThreatQ Identities

Identity-1

ThreatQ Incident

Incident-1, Incident-1

ThreatQ Intrusion Set

Intrusion Set-1, Intrusion set-1

ThreatQ Malware

MacDef, MacSpy, Mafalda

ThreatQ Signatures

Test Signature: Test Signature

ThreatQ Tools

Tasklist, Tool-1, Tor

ThreatQ TTP

ttp1, TTP-1

ThreatQ Vulnerability

Vulnerability-1, Vulnerability-1

ThreatQ Description

Added Description For Testing

Delete



ThreatQ Comments will not be populated in worknotes if enrichment is executed from an observable table.

Auto Observable Enrichment

Auto Observable Enrichment can be performed on an observable by attaching it to a security incident.

SETTING

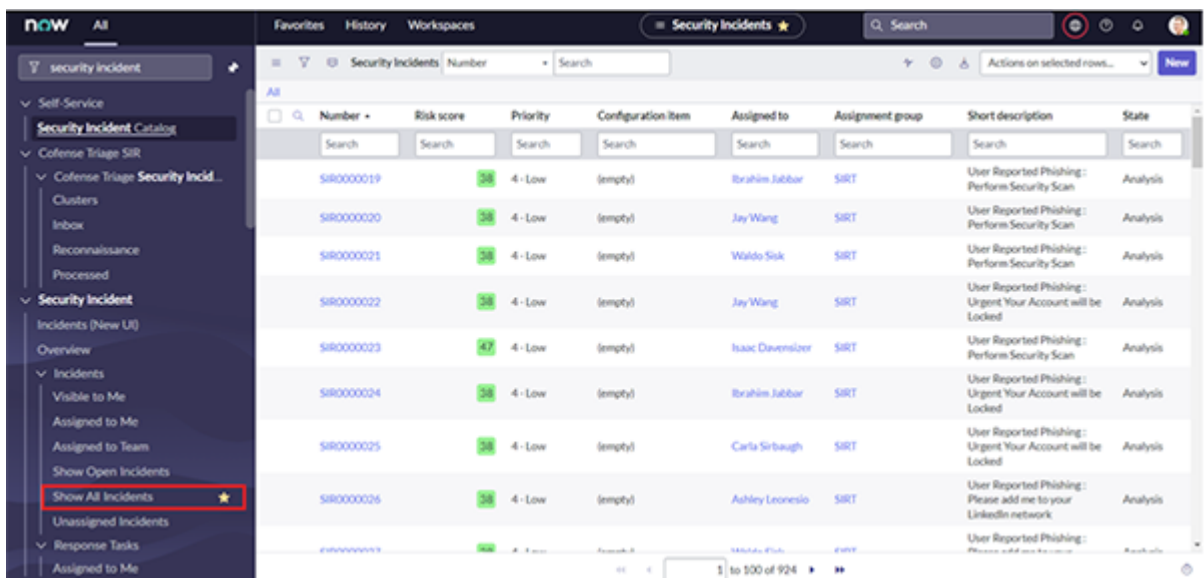
Role admin
Required

DETAILS

Prerequisites Set **Observable Enrichment Results** as the input in the TQ Attribute Location.

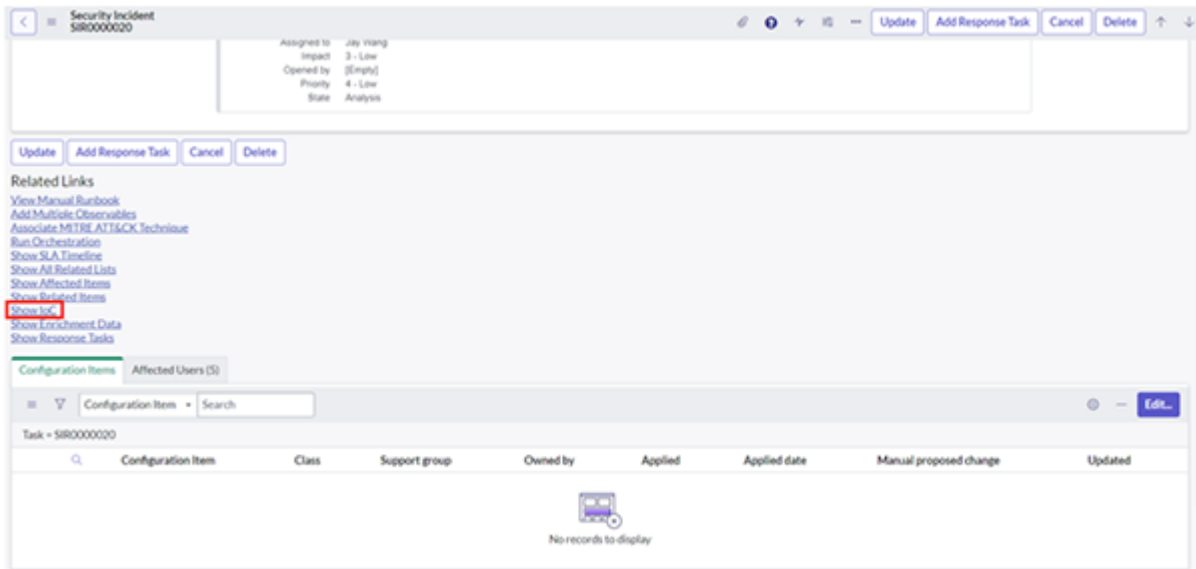
Performing Auto Observable Enrichment:

1. Navigate to **Security Incident > Incidents > Show All Incidents**.



Number	Risk score	Priority	Configuration item	Assigned to	Assignment group	Short description	State
SIR0000019	38	4 - Low	(empty)	Ibrahim Jabbar	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000020	38	4 - Low	(empty)	Jay Wang	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000021	38	4 - Low	(empty)	Waldo Sisk	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000022	38	4 - Low	(empty)	Jay Wang	SIRT	User Reported Phishing: Urgent Your Account will be Locked	Analysis
SIR0000023	47	4 - Low	(empty)	Isaac Davenport	SIRT	User Reported Phishing: Perform Security Scan	Analysis
SIR0000024	38	4 - Low	(empty)	Ibrahim Jabbar	SIRT	User Reported Phishing: Urgent Your Account will be Locked	Analysis
SIR0000025	38	4 - Low	(empty)	Carla Sirbaugh	SIRT	User Reported Phishing: Urgent Your Account will be Locked	Analysis
SIR0000026	38	4 - Low	(empty)	Ashley Leoncio	SIRT	User Reported Phishing: Please add me to your LinkedIn network	Analysis

2. Click on the security incident that the observable is linked to and then click on **Show IOC** under the *Related Links* section.



3. Click **New**, located under the *Associated Observables* section, to create a new observable. Link the observable to the security incident or click **Edit** to add links an existing observable.

Security Incident SIRO000020

Associated Observables (17) Security Scan Requests

Observable	Observable type	Context	Finding	Incident count	MITRE ATT&CK Information	Updated
67.231.157.3	IP address (V4)	(empty)	Unknown	13		2019-09-03 23:06:09
matthegrey0@gmail.com	Email address	(empty)	Unknown	11		2019-09-03 23:06:09
8.16.0.36	IP address (V4)	(empty)	Unknown	7		2019-09-03 23:06:09
A82B794C9694AFD69EDAA804C3188A89723DA6...	SHA256 hash	(empty)	Unknown	9		2019-09-03 23:06:09
8.16.0.42	IP address (V4)	(empty)	Unknown	14		2019-09-03 22:54:17
209.85.166.68	IP address (V4)	(empty)	Unknown	4		2019-08-30 00:08:12
2603.1066.404b9c34	IP address (V6)	(empty)	Unknown	2		2019-08-29 01:35:24
Perform Security Scan	Email subject	(empty)	Unknown	4		2019-08-28 04:27:34
CAGcQpPawVoxYB9AwOCcwTH9Q2+KGCOSGa3ZH...	Email Message ID	(empty)	Unknown	3		2019-08-28 04:07:01
10.152.82.87	IP address (V4)	(empty)	Unknown	1		2019-08-28 04:04:01
2a01:111:4000:7e49:205	IP address (V6)	(empty)	Unknown	1		2019-08-28 04:04:01

Add Filter Run filter

-- choose field -- -- oper -- -- value --

Collection

0006eaf451d762e16d900ebfc915920a
0014288287a4e49e2786ca2be09f1c8a
0014bc78848db9f6665d72057a5abca
001536c46b2b053c569bc78112507a72
0032a9635396ecDeb5b04883d71b087
00334a4def120130663f58f3589b6087
003927a9466db3714e046444bad5a76
004244709748e3ada33d78607b5ced6
00424e87b9f44d7513eac14760dec1a1
0043c39e24590149441fba48091caaf
006741ee01a0058ca196ab8d1sc0f7
00a15326a6f884906de2a708b5b6c8d2bbfad69
01b1e0f46ca45319742887e566d7eeb
028591d79115587ad3c8d25e9b777f768
02a485ac38b8ca12c5f96d7bdeff9f1
07a6a6af1b1f1844530b676c4818f5a...

Associated Observables List

SIRO000020

10.152.82.87
127.0.0.1
209.85.166.68
2603.1066.404b9c34
2603.1066.4052a:19
2603.1066.805f5:15
2a01:111:4000:7e49:205
67.231.157.3
8.16.0.36
8.16.0.42
A82B794C9694AFD69EDAA804C3188A89723C
ac7886f557a7e383c7bd66817318fb432411653c
CAGcQpPawVoxYB9AwOCcwTH9Q2+KGCOSGa3
https://us1.defense.proofpoint.com/v2/ur/ta=https-3A
https://us1.defense.proofpoint.com/v2/ur/ta=https-3A
matthegrey0@gmail.com
DuckDuckGo DuckDuckGo

Cancel Save

Once the observable is linked to the incident, auto threat lookup is started.

Security Incident SIRO000020

Hi Team,

Dear user, Our anti-malware scanner has detected 5 trojan viruses on your device today. This may cause your device to shut down or loss of critical data. To protect your device and data, visit this link to perform a security scan. Thank you, The Corporate IT Security Team.

To perform security scan on in your system provide your acceptance. For more details refer attached Reference manuals.

Work notes

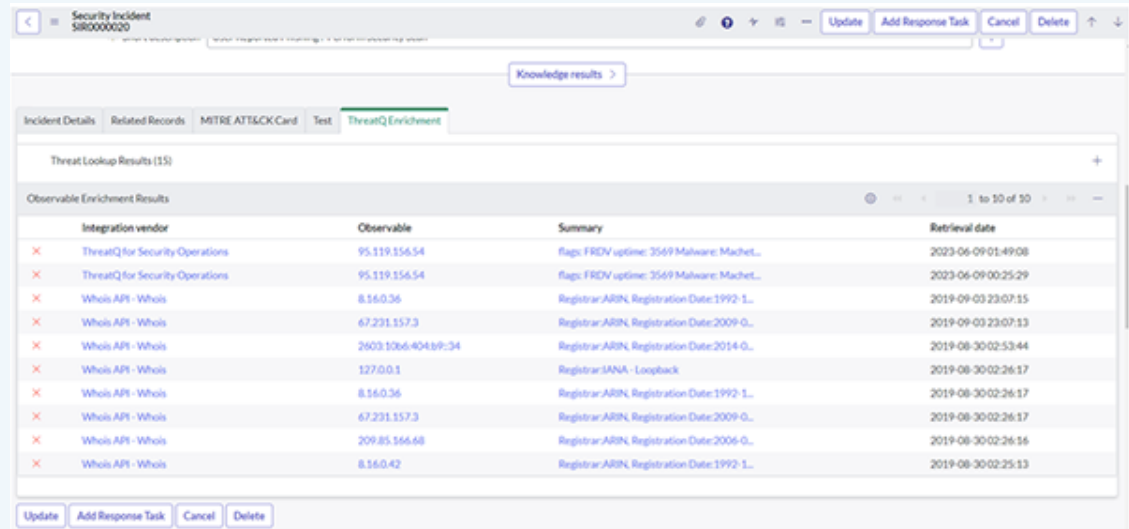
Activities: 32

- System Automation activity • 2023-06-09 01:49:08
Workflow [Security Operations Integration - Enrich Observable](#) execution completed.
Finished running Enrich observable capability
- System Automation activity • 2023-06-09 01:49:02
Workflow [Security Operations Integration - Enrich Observable](#) execution started.
Data inputs for this action: 95.102.156.54
- System Automation activity • 2023-06-09 01:48:51
Workflow [Security Incident Response - Create IoC Lookup Request for IoC Changes](#) execution started.
Data inputs for this action:



Worknotes will be generated in the **Incident Details** tab.

Threat Lookup Results can also be accessed via the **ThreatQ Enrichment** tab.



Knowledge results >

Incident Details Related Records MITRE ATT&CK Card Test **ThreatQ Enrichment**

Threat Lookup Results (15)

Observable Enrichment Results 1 to 10 of 10

Integration vendor	Observable	Summary	Retrieval date
ThreatQ for Security Operations	95.119.156.54	Flags: FRD/V uptime: 3569 Malware: Machet...	2023-06-09 01:49:08
ThreatQ for Security Operations	95.119.156.54	Flags: FRD/V uptime: 3569 Malware: Machet...	2023-06-09 00:25:29
Whois API - Whois	8.16.0.36	Registrar: ARIN, Registration Date: 1992-1...	2019-09-03 23:07:15
Whois API - Whois	67.231.157.3	Registrar: ARIN, Registration Date: 2009-0...	2019-09-03 23:07:13
Whois API - Whois	2603.1066.404.b9-34	Registrar: ARIN, Registration Date: 2014-0...	2019-08-30 02:53:44
Whois API - Whois	127.0.0.1	Registrar: IANA - Loopback	2019-08-30 02:26:17
Whois API - Whois	8.16.0.36	Registrar: ARIN, Registration Date: 1992-1...	2019-08-30 02:26:17
Whois API - Whois	67.231.157.3	Registrar: ARIN, Registration Date: 2009-0...	2019-08-30 02:26:17
Whois API - Whois	209.85.166.68	Registrar: ARIN, Registration Date: 2006-0...	2019-08-30 02:26:16
Whois API - Whois	8.16.0.42	Registrar: ARIN, Registration Date: 1992-1...	2019-08-30 02:25:13

Update Add Response Task Cancel Delete

- Open the observable enrichment results and click on the **hamburger icon**, located to the top left, and select **View > ThreatQ** to view the details of the observable.



Observable Enrichment Result 95.119.156.54 View: ThreatQ

Observable: 95.119.156.54 Retrieval date: 2023-06-09 00:25:29

ThreatQ Score: 8 Integration vendor: ThreatQ for Security Operations

ThreatQ Status: Active ThreatQ Type: IP Address

ThreatQ Created Date: 2023-06-07 16:01:19 ThreatQ Last Modified Date: 2023-06-08 06:42:44

Summary: Flags: FRD/V uptime: 3569 Malware: Machete, MacSpy, Malafida Adversaries: admin@338, Ajax Security Team, AjaxTM

Raw data:

```
{
  "asset": {
    "created_at": "2023-06-07 05:56:43",
    "description": null,
    "id": 1,
    "object_code": "asset",
    "object_id": 11,
    "object_name": "Assets",
    "object_name_plural": "Assets",
    "pivot": {
      "created_at": "2023-06-08 06:45:56",
      "id": 34205,
      "updated_at": "2023-06-08 06:45:56"
    },
    "status": null,
    "touch_at": "2023-06-08 10:21:25",
    "type": null,
    "updated_at": "2023-06-07 05:56:43",
    "value": "asset 1"
  },
  "created_at": "2023-06-07 11:19:59",
  "name": null
}
```

ThreatQ Attributes: Flags: FRD/V uptime: 3569

Observable Enrichment Result
95.119.156.54 View ThreatQ

{"created_at":"2023-06-07 11:19:59",
"description":"null"}

ThreatQ Attributes

ThreatQ Sources

ThreatQ Tags

ThreatQ Adversaries

ThreatQ Asset

ThreatQ Attack Pattern

ThreatQ Campaign

ThreatQ Course Of Action

ThreatQ Events

ThreatQ Exploit Target

Flags: FRDV
uptime: 2569

www.dan.me.uk Tor Node List, Crest

Test tag1, Test tag2, demo1

admin@338, Ajax Security Team, AjaxTM

asset 1, asset 2, Asset-1

Attack pattern 2, Attack Pattern-1

C0011, C0018

action 1, action 2, action 3

SECC0001011 - ANZ Test, SECC0001012 - Adversary Cricket1 has gained access to the grain silos, SECC0001014 - dev app

Exploit Target1, Exploit Target-1

Observable Enrichment Result
95.119.156.54 View ThreatQ

ThreatQ Identities

ThreatQ Incident

ThreatQ Intrusion Set

ThreatQ Malware

ThreatQ Signatures

ThreatQ Tools

ThreatQ TTP

ThreatQ Vulnerability

Identity-1

Incident1, Incident-1

Intrusion Set1, Intrusion set-1

Machete, MacSpy, Mafalda

Test Signature: Test Signature

Tasklist, Tool-1, Tor

http5, TTP-1

Vulnerability1, Vulnerability-1

ThreatQ Description Add Description For Testing

Delete



If there are any ThreatQ comments for the observable then worknotes will be updated with ThreatQ comments.

Activities: 250

System

Workflow [Security Operations Integration - Enrich Observable](#) execution completed.
Finished running Enrich observable capability

Automation activity • 2023-06-14 00:22:08 4m ago

System

[ThreatQ] Comments for observable "95.119.156.54".
Test comment1, Test comment2

Work notes • 2023-06-14 00:22:07 4m ago

System


Workflow [Security Operations Integration - Enrich Observable](#) execution started.
Data inputs for this action: [95.119.156.54](#)

Automation activity • 2023-06-14 00:22:00 4m ago

Troubleshooting

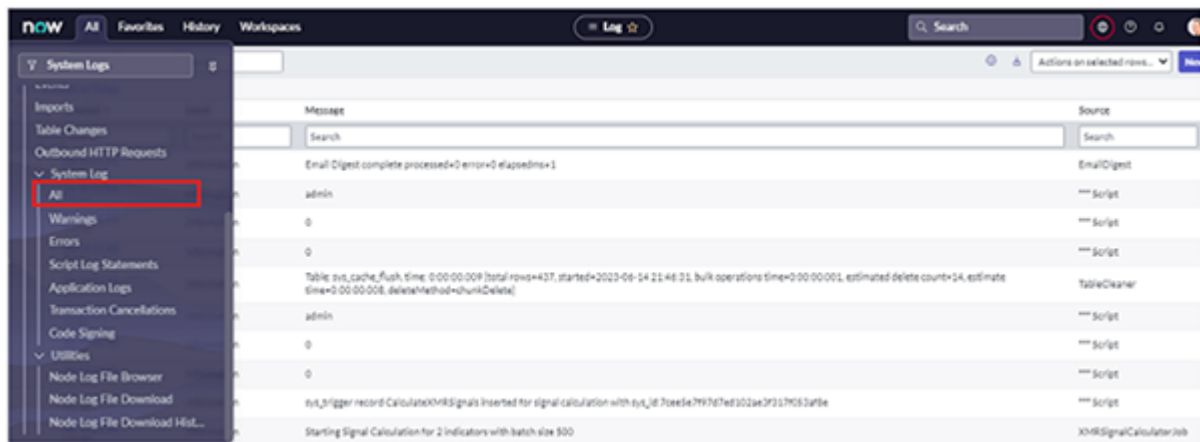
Increase Field of Input Field

The default max for characters used in object properties and attribute fields is 200. The steps below detail how to increase that limit.

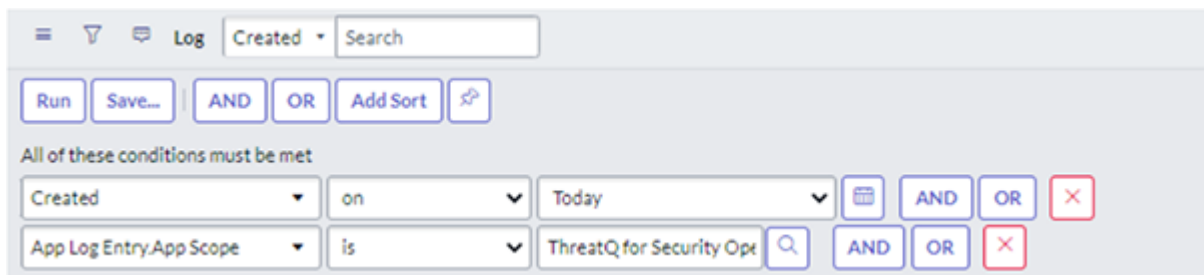
1. Open the `sn_sec_core_integration_item_config` table using the `sn_sec_core_integration_item_config.list` command in the navigation panel.
2. Click on the  icon on the left side and open **Configure -> Table**.
3. Click on the **Here** link if you receive the following message: "This record is in the Global application, but ThreatQ for Security Operations is the current application. To edit this record click here."
4. Search for the value named column in the columns list provided in the columns tab.
5. Update the **Max Length** to 500 or the required length based on your data for the value field.
6. Click on the **Update**.

Application Logs

1. Navigate to **System Logs -> All**.



2. To display application-specific logs apply the following filter displayed in the image below.



Upgrading Application

Perform the following steps when upgrading the application from a previous version.



The user needs to reconfigure credentials in the Integration Tile after the application has been upgraded.

Data that has already been enriched wouldn't have values in the newly created fields. These can be seen data in the Default View.

1. Log in to the instance.
2. Navigate to **System Applications > All Available Applications > All**.
3. Find the application with the filter criteria and search bar.
4. Next to the application listing, select the version to install.
5. Click **Update**.



Existing workflow activity will not be affected by the Upgrade process.

Known Issues / Limitations

- The Hash Observable Type record in the observable enrichment under the ThreatQ Enrichment tab will not get populated in the Security Incident.

Change Log

- **Version 1.2.0**
 - Added to the app configuration page the ability to enter a comma-separated list of observables relationships to be ingested from ThreatQ: Adversaries, Asset, Attack Pattern, Campaign, Course of Action, Exploit Target, Events, Identity, Incident, Intrusion Set, Malware, Signatures, Type, TTP, Tool, Vulnerability.
 - Added to the app configuration page the ability to enter a comma-separated list of ThreatQ attribute names to be ingested during the enrichment.
 - Added to the app configuration page the ability to enter a comma-separated list of observable properties' names to be ingested from ThreatQ during enrichment: Type, Status, Score, Sources, Tags.
 - Added separate columns in ServiceNow to store each object artifact (Tags, Comments, Description, Status, Attributes, Score, Sources and relationships) that has been ingested from ThreatQ.
 - Updated the format of the ThreatQ score from string to integer.
 - Updated the format of the Created Date and Modified Date from string to a date format.
 - Validated the app for the Utah release.
 - Updated minimum ThreatQ version to 5.16.0.
- **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