

ThreatQuotient



ServiceNow CDF

Version 2.0.0

June 25, 2024

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
Installation.....	8
Configuration	9
Security Incidents Parameters	9
Security Cases Parameters	13
Security Incident Response Task Parameters.....	15
Service Desk Incidents Parameters	17
Observable Parameters	19
ThreatQ Mapping.....	21
ServiceNow Security Incidents	21
ServiceNow Security Cases.....	27
ServiceNow Security Incident Response Task.....	31
ServiceNow Service Desk Incidents	36
ServiceNow Observables	43
ServiceNow Observable Type to ThreatQ Indicator Type.....	45
Get Related Observables Supplemental.....	48
Get Object By Link Supplemental	49
Get Related Threat Actors Supplemental	50
Get Related Intrusion Sets Supplemental	51
Get Journal Entries Supplemental	52
Average Feed Run.....	53
ServiceNow Security Incidents	53
ServiceNow Security Cases.....	54
ServiceNow Security Incident Response Task.....	54
ServiceNow Service Desk Incidents	55
ServiceNow Observables	55
Change Log	56

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 © 2024 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 Integration Version	2.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

ServiceNow is an incident response & workflow platform that allows users to create, track, and manage incidents across their entire business.

The ServiceNow CDF for ThreatQ enables the automatic ingestion of tickets & their context from ServiceNow, into ThreatQ.

The integration provides the following feeds:

- **ServiceNow Security Incidents** - ingests Security Incidents from ServiceNow's Security Incident Response (SIR) module.
- **ServiceNow Security Cases** - ingests Security Cases from ServiceNow's Threat Intelligence (TI) module.
- **ServiceNow Security Incident Response Task** - ingests incident response tasks from ServiceNow's Security Incident Response module into ThreatQ.
- **ServiceNow Service Desk Incidents** - ingests service desk incidents from ServiceNow into ThreatQ.
- **ServiceNow Observables** - ingests observables from ServiceNow's Threat Intelligence module into ThreatQ as indicators.

The integration ingests the following system objects:

- Adversaries
- Attack Patterns
- Incidents
- Indicators
- Malware
- Tools

Prerequisites

The following is required to install and run the integration:

- A ServiceNow instance with the Security Incident Response (SIR) module enabled (Security Incidents feed).
- A ServiceNow instance with the Threat Intelligence (TI) module enabled (Security Cases feed).
- The **ServiceNow Security Incidents plugin** be installed in your ServiceNow instance/environment. Failure to do so will result in the integration not ingesting alerts.
- Your ServiceNow username and password.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

Configuration



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

To configure the integration:


1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).







If you are installing the integration for the first time, it will be located under the **Disabled** tab.


3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Security Incidents Parameters




PARAMETER	DESCRIPTION
ServiceNow Host	Your hostname for your ServiceNow instance.
ServiceNow Username	You ServiceNow username that will be used to authenticate with the ServiceNow API. <div>  This account should have the appropriate permissions to access the ServiceNow API. </div>
ServiceNow Password	The password associated with the username above.
Date Field	Select the date field to use to filter results from ServiceNow. Options include: <ul style="list-style-type: none"> ◦ Created At ◦ Updated At (default)


PARAMETER	DESCRIPTION
	<div>  <p>The Updated At option may overwrite existing tickets in ThreatQ based on the current ServiceNow context for a given incident.</p> </div>
Custom Sysparm Query	Optional - add conditions to query. This query must follow ServiceNow's query syntax - see ServiceNow's documentation for more details - https://docs.servicenow.com/bundle/vancouver-platform-user-interface/page/use/common-ui-elements/reference/r_OpAvailableFiltersQueries.html .
Fetch Journal Entries	<p>When enabled, the integration will fetch journal entries for each incident. The entries include work notes, comments, and other automation activities. This parameter is enabled by default.</p> <div>  <p>Enabling this will add +1 API calls per incident.</p> </div>
Ingest Parent Security Incident	<p>Select whether to ingest the parent security incident, if it is available.</p> <div>  <p>Enabling this will add +1 API calls per incident.</p> </div>
Fetch Relationships	<p>Select the relationships to fetch for each incident.</p> <div>  <p>Each selected relationship will add +1 API calls per object.</p> </div>
Related Observable Type Filter	<p>Select the observable type to ingest from Related Observables. Options include:</p> <ul style="list-style-type: none"> ◦ Unknown (String) ◦ Email Address ◦ Email Subject ◦ MD5 (default) ◦ SHA-1 ◦ SHA-256 (default) ◦ SHA-384 ◦ CIDR Block (default) ◦ MAC Address ◦ FQDN (default) ◦ Hostname (default) ◦ URL (default) ◦ URI ◦ CVE (default)

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ SHA-512 ◦ File Path ◦ IPv4 Address (default) ◦ IPv6 Address (default) ◦ Username ◦ Mutex ◦ ASN
Save ServiceNow Security Incident As	Select how to save the ServiceNow incident in ThreatQ. Options include Incident and Event .
Incident Context	<p>Select the incident context to bring in from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ ServiceNow URL ◦ Created By ◦ Opened At ◦ Opened By ◦ Contact Type ◦ Tags ◦ Is Active ◦ Activity Due ◦ Approval Status ◦ Assigned To ◦ Assignment Group ◦ Caller ◦ Attack Vector ◦ Business Criticality ◦ Category ◦ Subcategory ◦ Closed At ◦ Close Code ◦ Close Notes ◦ Closed By ◦ Confidence Score ◦ Impact ◦ Location ◦ Priority ◦ Risk ◦ Risk Score ◦ Risk Change ◦ Severity ◦ Urgency ◦ Escalation Status ◦ State ◦ Substate ◦ Affected Platform ◦ Hold Reason ◦ Expected Start ◦ Expected End ◦ Affected User ◦ Estimated End ◦ SLA Suspended ◦ SLA Suspended On ◦ SLA Suspended For ◦ Made SLA ◦ Spam ◦ Is Catalog ◦ Risk Score Override ◦ Department ◦ Upon Reject ◦ Upon Approval
Incident MITRE Context	Select the incident relationships to bring in from ServiceNow. Options include:

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ MITRE ATT&CK Techniques ◦ MITRE Tactics ◦ Malware ◦ Tools ◦ Threat Actors <div>  <p>ServiceNow automatically extrapolates Malware, Adversary, and Tool relationships based on the related MITRE Attack Techniques. Enabling these relationships may bring unwanted connections into ThreatQ, use them with some caution.</p> </div>
Description Context	<p>Select the types you would like to ingest from the related observables. Options include:</p> <ul style="list-style-type: none"> ◦ Ticket Metadata ◦ Ticket Description ◦ Closure Information
Parse Journal Entries for Indicators	<p>Select the fields to parse for Indicators from the journal entries. This includes work notes, comments, and other automation activities. Options include:</p> <ul style="list-style-type: none"> ◦ Work Notes ◦ Comments ◦ Automation Activities
Parse Indicator Types	<p>Select the indicator types you would like to automatically parse from the content. Option include:</p> <ul style="list-style-type: none"> ◦ CVE ◦ IP Address ◦ IPv6 Address ◦ CIDR Block ◦ FQDN ◦ URL ◦ MD5 ◦ SHA-1 ◦ SHA-256 ◦ SHA-512 ◦ Email Address ◦ Registry Key
Normalization Options	<p>Select the normalization options you would like to use when parsing indicators from the content. Options include:</p> <ul style="list-style-type: none"> ◦ Normalize Indicators (default) ◦ Derive FQDNs from URLs


Security Cases Parameters




PARAMETER	DESCRIPTION
ServiceNow Host	Your hostname for your ServiceNow instance.
ServiceNow Username	<p>You ServiceNow username that will be used to authenticate with the ServiceNow API.</p> <div>  This account should have the appropriate permissions to access the ServiceNow API. </div>
ServiceNow Password	The password associated with the username above.
Date Field	<p>Select the date field to use to filter results from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ Created At ◦ Updated At (default) <div>  The Updated At option may overwrite existing tickets in ThreatQ based on the current ServiceNow context for a given incident. </div>
Custom Sysparm Query	<p>Optional - add conditions to query. This query must follow ServiceNow's query syntax - see ServiceNow's documentation for more details - https://docs.servicenow.com/bundle/vancouver-platform-user-interface/page/use/common-ui-elements/reference/r_OpAvailableFiltersQueries.html.</p>
Fetch Journal Entries	<p>When enabled, the integration will fetch journal entries for each incident. The entries include work notes, comments, and other automation activities. This parameter is enabled by default.</p> <div>  Enabling this will add +1 API calls per incident. </div>

PARAMETER	DESCRIPTION
Fetch Relationships	<p>Select the relationships to fetch for each case.</p> <div>  Each selected relationship will add +1 API calls per object. </div>
Related Observable Type Filter	<p>Select the observable type to ingest from Related Observables. Options include:</p> <ul style="list-style-type: none"> ◦ Unknown (String) ◦ Email Address ◦ Email Subject ◦ MD5 (default) ◦ SHA-1 ◦ SHA-256 (default) ◦ SHA-384 ◦ SHA-512 ◦ File Path ◦ IPv4 Address (default) ◦ IPv6 Address (default) ◦ CIDR Block (default) ◦ MAC Address ◦ FQDN (default) ◦ Hostname (default) ◦ URL (default) ◦ URI ◦ CVE (default) ◦ Username ◦ Mutex ◦ ASN
Save ServiceNow Security Case As	<p>Select how to save the ServiceNow Case in ThreatQ. Options include Incident and Event.</p>
Case Context	<p>Select the case context to bring in from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ ServiceNow URL ◦ Created By ◦ Opened At ◦ Opened By ◦ Contact Type ◦ Tags ◦ Is Active ◦ Activity Due ◦ Approval Status ◦ Assigned To ◦ Assignment Group ◦ Caller ◦ Risk ◦ Risk Score ◦ Risk Change ◦ Severity ◦ Urgency ◦ Escalation Status ◦ State ◦ Substate ◦ Affected Platform ◦ Hold Reason ◦ Expected Start ◦ Expected End

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Attack Vector ◦ Business Criticality ◦ Category ◦ Subcategory ◦ Closed At ◦ Close Code ◦ Close Notes ◦ Closed By ◦ Confidence Score ◦ Impact ◦ Location ◦ Priority ◦ Affected User ◦ Estimated End ◦ SLA Suspended ◦ SLA Suspended On ◦ SLA Suspended For ◦ Made SLA ◦ Spam ◦ Is Catalog ◦ Risk Score Override ◦ Department ◦ Upon Reject ◦ Upon Approval
Description Context	Select the types you would like to ingest from the related observables. Options include: <ul style="list-style-type: none"> ◦ Ticket Metadata ◦ Ticket Description ◦ Closure Information


Security Incident Response Task Parameters




PARAMETER	DESCRIPTION
ServiceNow Host	Your hostname for your ServiceNow instance.
ServiceNow Username	You ServiceNow username that will be used to authenticate with the ServiceNow API. <div>  This account should have the appropriate permissions to access the ServiceNow API. </div>
ServiceNow Password	The password associated with the username above.

PARAMETER	DESCRIPTION
Date Field	<p>Select the date field to use to filter results from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ Created At ◦ Updated At (default) <div>  The Updated At option may overwrite existing tickets in ThreatQ based on the current ServiceNow context for a given incident. </div>
Custom Sysparm Query	<p>Optional - add conditions to query. This query must follow ServiceNow's query syntax - see ServiceNow's documentation for more details - https://docs.servicenow.com/bundle/vancouver-platform-user-interface/page/use/common-ui-elements/reference/r_OpAvailableFiltersQueries.html.</p>
Ingest Parent Incident	<p>Select whether to ingest the parent incident, if it is available.</p> <div>  Enabling this will add +1 API calls per incident. </div>
Fetch Relationships	<p>Select the relationships to fetch for each incident.</p> <div>  Each selected relationship will add +1 API calls per object. </div>
Save ServiceNow Security Incidents As	<p>Select how to save the ServiceNow Security Incidents in ThreatQ. Options include Incident and Event.</p>
Incident Context	<p>Select the Security Incident context to bring in from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ ServiceNow URL ◦ Created By ◦ Opened At ◦ Opened By ◦ Contact Type ◦ Risk ◦ Risk Score ◦ Risk Change ◦ Severity ◦ Urgency

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Tags ◦ Is Active ◦ Activity Due ◦ Approval Status ◦ Assigned To ◦ Assignment Group ◦ Caller ◦ Attack Vector ◦ Business Criticality ◦ Category ◦ Subcategory ◦ Closed At ◦ Close Code ◦ Close Notes ◦ Closed By ◦ Confidence Score ◦ Impact ◦ Location ◦ Priority
	<ul style="list-style-type: none"> ◦ Escalation Status ◦ State ◦ Substate ◦ Affected Platform ◦ Hold Reason ◦ Expected Start ◦ Expected End ◦ Affected User ◦ Estimated End ◦ SLA Suspended ◦ SLA Suspended On ◦ SLA Suspended For ◦ Made SLA ◦ Spam ◦ Is Catalog ◦ Risk Score Override ◦ Department ◦ Upon Reject ◦ Upon Approval

Service Desk Incidents Parameters

PARAMETER	DESCRIPTION
ServiceNow Host	Your hostname for your ServiceNow instance.
ServiceNow Username	<p>You ServiceNow username that will be used to authenticate with the ServiceNow API.</p> <div>  <p>This account should have the appropriate permissions to access the ServiceNow API.</p> </div>
ServiceNow Password	The password associated with the username above.

PARAMETER	DESCRIPTION
Date Field	<p>Select the date field to use to filter results from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ Created At ◦ Updated At (default) <div>  The Updated At option may overwrite existing tickets in ThreatQ based on the current ServiceNow context for a given incident. </div>
Custom Sysparm Query	<p>Optional - add conditions to query. This query must follow ServiceNow's query syntax - see ServiceNow's documentation for more details - https://docs.servicenow.com/bundle/vancouver-platform-user-interface/page/use/common-ui-elements/reference/r_OpAvailableFiltersQueries.html.</p>
Ingest Parent Incident	<p>Select whether to ingest the parent incident, if it is available.</p> <div>  Enabling this will add +1 API calls per incident. </div>
Fetch Relationships	<p>Select the relationships to fetch for each incident.</p> <div>  Each selected relationship will add +1 API calls per object. </div>
Save ServiceNow Service Desk Incidents As	<p>Select how to save the ServiceNow Service Desk Incidents in ThreatQ. Options include Incident and Event.</p>
Incident Context	<p>Select the Service Desk Incident context to bring in from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ ServiceNow URL ◦ Created By ◦ Opened At ◦ Opened By ◦ Contact Type ◦ Risk ◦ Risk Score ◦ Risk Change ◦ Severity ◦ Urgency

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Tags ◦ Is Active ◦ Activity Due ◦ Approval Status ◦ Assigned To ◦ Assignment Group ◦ Caller ◦ Attack Vector ◦ Business Criticality ◦ Category ◦ Subcategory ◦ Closed At ◦ Close Code ◦ Close Notes ◦ Closed By ◦ Confidence Score ◦ Impact ◦ Location ◦ Priority
	<ul style="list-style-type: none"> ◦ Escalation Status ◦ State ◦ Substate ◦ Affected Platform ◦ Hold Reason ◦ Expected Start ◦ Expected End ◦ Affected User ◦ Estimated End ◦ SLA Suspended ◦ SLA Suspended On ◦ SLA Suspended For ◦ Made SLA ◦ Spam ◦ Is Catalog ◦ Risk Score Override ◦ Department ◦ Upon Reject ◦ Upon Approval



**Description
Context**

Select the types you would like to ingest from the related observables. Options include:

- Ticket Metadata
- Ticket Description
- Closure Information

Observable Parameters

PARAMETER	DESCRIPTION
ServiceNow Host	Your hostname for your ServiceNow instance.
ServiceNow Username	You ServiceNow username that will be used to authenticate with the ServiceNow API.

PARAMETER	DESCRIPTION
	<div>  This account should have the appropriate permissions to access the ServiceNow API. </div>
ServiceNow Password	The password associated with the username above.
Date Field	<p>Select the date field to use to filter results from ServiceNow. Options include:</p> <ul style="list-style-type: none"> ◦ Created At ◦ Updated At (default) <div>  The Updated At option may overwrite existing tickets in ThreatQ based on the current ServiceNow context for a given incident. </div>
Custom Sysparm Query	<p>Optional - add conditions to query. This query must follow ServiceNow's query syntax - see ServiceNow's documentation for more details - https://docs.servicenow.com/bundle/vancouver-platform-user-interface/page/use/common-ui-elements/reference/r_OpAvailableFiltersQueries.html.</p>

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

ServiceNow Security Incidents

The ServiceNow Security Incidents feed ingests incidents from ServiceNow's Security Incident Response module into ThreatQ.

Included with each incident will be the following:

- Related Observables
- Related Adversaries
- Related Malware
- Related Attack Patterns
- Related Tools
- Work Notes, Comments, & Automated Activities

GET https://{sub-domain}.service-now.com/api/now/v1/table/sn_si_incident

Sample Response:

```
{
  "result": [
    {
      "parent": "",
      "sla_suspended_reason": null,
      "watch_list": "",
      "upon_reject": "Cancel all future Tasks",
      "sys_updated_on": "2022-08-31 12:31:57",
      "qualification_group": "",
      "expected_end": "",
      "approval_history": "",
      "source_ip": "",
      "skills": "",
      "number": "SIR0001758",
      "problem": "",
      "previous_agent": "",
      "state": "Recover",
      "sys_created_by": "si_admin",
      "template_workflow_invoked": "false",
      "knowledge": "false",
      "order": "",
      "phish_email": "",
      "cmdb_ci": {
        "display_value": "ny8500-nbxs09",
        "link": "https://dev63597.service-now.com/api/now/v1/table/cmdb_ci/55b37e80c0a8010e00028a1d1a14e2d7"
      },
      "delivery_plan": "",
      "contract": "",
      "impact": "1 - High",
      "active": "true",
      "work_notes_list": "",
      "priority": "1 - Critical",
      "sys_domain_path": "/",
      "sla_suspended": "false",
      "business_duration": "",
      "group_list": ""
    }
  ]
}
```

```

"special_access_write": "",
"dest_ip": "",
"mitre_platform": "Linux,macOS,Windows,Network",
"approval_set": "",
"risk_change": null,
"malware_url": "",
"universal_request": "",
"template": "",
"short_description": "staged attack",
"correlation_display": "",
"delivery_task": "",
"work_start": "",
"request_type": null,
"affected_user": "",
"other_ioc": "",
"additional_assignee_list": "",
"alert_sensor": "",
"assigned_vendor": "",
"service_offering": "",
"sys_class_name": "Security Incident",
"closed_by": "",
"follow_up": "",
"mitre_group": "G0007 (APT28),G0065 (Leviathan),G0132 (CostaRicto),G0116 (Operation
Wocao),G0085 (FIN4),G0016 (APT29),G0100 (Inception),G0115 (GOLD SOUTHFIELD),G0034 (Sandworm
Team),G0105 (DarkVishnya),G0120 (Evilnum),G0139 (TeamTNT),G0129 (Mustang Panda),G0076 (Thrip),G0014
(Night Dragon),G0094 (Kimsuky),G0080 (Cobalt Group),G0048 (RTM),G0008 (Carbanak),G0069
(MuddyWater)",
"sla_suspended_on": "",
"estimated_end": "",
"vendor_reference": "",
"reassignment_count": "1",
"assigned_to": {
  "display_value": "Val Osborne",
  "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/
7e82abf03710200044e0bfc8bcbe5d32"
},
"request_category": "",
"requested_due_by": "",
"mitre_malware": "S0604 (Industroyer),S0623 (Siloscape),S0438 (Attor),S0687 (Cyclops
Blink),S0641 (Kobalos),S0282 (MacSpy),S0386 (Ursnif),S0342 (GreyEnergy),S0281 (Dok),S0491
(StrongPity),S0276 (Keydnab),S0366 (WannaCry),S0384 (Dridex),S0554 (Egregor),S0601 (Hildegard),S0030
(Carbanak),S0148 (RTM),S0266 (TrickBot)",
"sla_suspended_for": "",
"business_criticality": "1 - Critical",
"sla_due": "UNKNOWN",
"opened_for": {
  "display_value": "System Administrator",
  "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/
6816f79cc0a8016401c5a33be04be441"
},
"comments_and_work_notes": "2022-08-29 15:30:05 - System Administrator (Work notes)\nRisk
score changed from 87 to 92 due to change in business impact\n\n2022-08-29 15:30:04 - System
Administrator (Work notes)\nRisk score changed from Empty to 87 due to user action to update all
risk scores\n\n",
"mitre_technique": "T1090.003 (Multi-hop Proxy),T1219 (Remote Access Software)",
"special_access_read": "",
"substate": "",
"escalation": "Normal",
"upon_approval": "Proceed to Next Task",
"correlation_id": "",
"asset": "",
"mitre_tool": "S0183 (Tor)",
"spam": "false",
"referrer_url": "",

```

```

"made_sla": "true",
"mitre_tactic": "TA0011 (Command and Control)",
"is_catalog": "false",
"malware_hash": "",
>alert_rule": "",
"task_effective_number": "SIR0001758",
"external_url": "",
"sys_updated_by": "admin",
"opened_by": {
  "display_value": "System Administrator",
  "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/
6816f79cc0a8016401c5a33be04be441"
},
"user_input": "",
"sys_created_on": "2022-08-09 06:34:13",
"sys_domain": {
  "display_value": "global",
  "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user_group/global"
},
"pir": null,
"route_reason": "",
"closed_at": "",
"business_service": "",
"attack_vector": "Attack Correlation",
"time_worked": "",
"expected_start": "2022-09-10 10:19:36",
"opened_at": "2022-08-09 06:34:13",
"task_created": "false",
"work_end": "",
"confidence_score": "",
"prediction": null,
"automation_activity": "",
"subcategory": "Vulnerable application",
"work_notes": "2022-08-29 15:30:05 - System Administrator (Work notes)\nRisk score changed
from 87 to 92 due to change in business impact\n\n2022-08-29 15:30:04 - System Administrator (Work
notes)\nRisk score changed from Empty to 87 due to user action to update all risk scores\n\n",
"security_tags": "",
"risk_score_override": "false",
"initiated_from": "",
"close_code": null,
"assignment_group": {
  "display_value": "Vulnerability Response",
  "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user_group/
9e1d0444ffa33100158bffffffffffffd"
},
"description": "Recon behavior (i.e. vulnerability scanning) detected from a data center
server. DB server was actively scanning other hosts in the data center.",
"calendar_duration": "",
"close_notes": "",
"pir_respondents": "Val Osborne",
"sys_id": "d8b6b953ff933100158bffffffffffff7f",
"contact_type": "Phone",
"urgency": "3 - Low",
"secure_notes": "",
"company": "",
"new_pir_respondents": "",
"department": "",
"activity_due": "UNKNOWN",
"severity": "1 - High",
"comments": "",
"risk_score": "92",
"approval": "Not Yet Requested",
"due_date": "",
"sys_mod_count": "22",

```

```

    "parent_security_incident": "",
    "sys_tags": "",
    "billable": "false",
    "mitre_data_source": "Network Traffic: Network Traffic Content,Network Traffic: Network
Connection Creation,Network Traffic: Network Traffic Flow,Process: Process Creation",
    "caller": "",
    "location": {
      "display_value": "450 Lexington Avenue, New York,NY",
      "link": "https://dev63597.service-now.com/api/now/v1/table/cm_location/
5f669b59c0a8010e00209343c0c6f9c1"
    },
    "risk": "Very High",
    "category": "Un-patched vulnerability",
    "incident": "",
    "change_request": "",
    "security_incident_self": ""
  }
]
}

```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the result list. Additional mappings are handled by the [ServiceNow Observables](#) feed. If the **Ingest Parent Security Incident** configuration option is enabled, the value `.parent_security_incident.link` is sent to **ServiceNow Get Object By Link** supplemental feed. The feed retrieves the parent incident that is processed the same as the current ingested incident.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.number,</code> <code>.short_description</code>	Incident/Event Value	N/A	<code>.sys_created_on</code>	SIR0001758 \ staged attack	N/A
<code>.security_tags</code>	Incident/Event Tag	N/A	N/A	TLP: RED	If enabled. Tags containing : are updated.
<code>.description</code>	Incident/Event Description	N/A	N/A	Recon behavior...	Concatenated with other values.
<code>.activity_due</code>	Incident/Event Attribute	Activity Due	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.mitre_platform</code>	Incident/Event Attribute	Affected Platform	<code>.sys_created_on</code>	N/A	If enabled.
<code>.affected_user</code>	Incident/Event Attribute	Affected User	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.approval</code>	Incident/Event Attribute	Approval Status	<code>.sys_created_on</code>	Not Yet Requested	If enabled. Updated at ingestion
<code>.assigned_to.display_value</code>	Incident/Event Attribute	Assigned To	<code>.sys_created_on</code>	John Doe	If enabled. Updated at ingestion
<code>.assignment_group.display_value</code>	Incident/Event Attribute	Assignment Group	<code>.sys_created_on</code>	Windows Security	If enabled. Updated at ingestion
<code>.attack_vector</code>	Incident/Event Attribute	Attack Vector	<code>.sys_created_on</code>	SQLi	If enabled.
<code>.business_criticality</code>	Incident/Event Attribute	Business Criticality	<code>.sys_created_on</code>	Critical	If enabled. Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.caller.display_value	Incident/Event Attribute	Caller	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.category	Incident/Event Attribute	Category	.sys_create_d_on	Unauthorized access	If enabled. Updated at ingestion
.close_code	Incident/Event Attribute	Close Code	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.close_notes	Incident/Event Attribute	Close Note	.sys_create_d_on	Solved	If enabled
.closed_at	Incident/Event Attribute	Closed At	.sys_create_d_on	N/A	If enabled
.closed_by.display_value	Incident/Event Attribute	Closed By	.sys_create_d_on	N/A	If enabled
.confidence_score	Incident/Event Attribute	Confidence Score	.sys_create_d_on	55	If enabled. Updated at ingestion
.contact_type	Incident/Event Attribute	Contact Type	.sys_create_d_on	Phone	If enabled. Updated at ingestion
.sys_created_by	Incident/Event Attribute	Created By	.sys_create_d_on	si_admin	If enabled.
.department	Incident/Event Attribute	Department	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.escalation	Incident/Event Attribute	Escalation Status	.sys_create_d_on	Normal	If enabled. Updated at ingestion
.estimated_end	Incident/Event Attribute	Estimated End	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.expected_end	Incident/Event Attribute	Expected End	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.expected_start	Incident/Event Attribute	Expected Start	.sys_create_d_on	2022-09-10 10:19:36	If enabled. Updated at ingestion
.hold_reason	Incident/Event Attribute	Hold Reason	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.impact	Incident/Event Attribute	Impact	.sys_create_d_on	High	If enabled. Updated at ingestion
.active	Incident/Event Attribute	Is Active	.sys_create_d_on	true	If enabled. Updated at ingestion
.is_catalog	Incident/Event Attribute	Is Catalog	.sys_create_d_on	false	If enabled. Updated at ingestion
.location.display_value	Incident/Event Attribute	Location	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.made_sla	Incident/Event Attribute	Made SLA	.sys_create_d_on	true	If enabled. Updated at ingestion
.opened_at	Incident/Event Attribute	Opened At	.sys_create_d_on	2022-08-09 06:34:13	If enabled. Updated at ingestion
.opened_by	Incident/Event Attribute	Opened By	.sys_create_d_on	System Administrator	If enabled. Updated at ingestion
.priority	Incident/Event Attribute	Priority	.sys_create_d_on	Critical	If enabled. Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.risk	Incident/Event Attribute	Risk	.sys_create_d_on	Very High	If enabled. Updated at ingestion
.risk_change	Incident/Event Attribute	Risk Change	.sys_create_d_on	Up	If enabled. Updated at ingestion
.risk_score	Incident/Event Attribute	Risk Score	.sys_create_d_on	40	If enabled. Updated at ingestion
.risk_score_override	Incident/Event Attribute	Risk Score Override	.sys_create_d_on	false	If enabled. Updated at ingestion
.sys_id	Incident/Event Attribute	ServiceNow Link	.sys_create_d_on	N/A	If enabled. Concatenated with host. Updated at ingestion
.severity	Incident/Event Attribute	Severity	.sys_create_d_on	Medium	If enabled. Updated at ingestion
.sla_suspended	Incident/Event Attribute	SLA Suspended	.sys_create_d_on	false	If enabled. Updated at ingestion
.sla_suspended_for	Incident/Event Attribute	SLA Suspended For	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.sla_suspended_on	Incident/Event Attribute	SLA Suspended On	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.spam	Incident/Event Attribute	Spam	.sys_create_d_on	false	If enabled. Updated at ingestion
.state	Incident/Event Attribute	State	.sys_create_d_on	Closed	If enabled. Updated at ingestion
.subcategory	Incident/Event Attribute	Subcategory	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.substate	Incident/Event Attribute	Substate	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.number	Incident/Event Attribute	System Number	.sys_create_d_on	SIR0001758	If enabled. Updated at ingestion
.tactic	Incident/Event Attribute	Tactic	.sys_create_d_on	Reconnaissance	If enabled.
.upon_approval	Incident/Event Attribute	Upon Approval	.sys_create_d_on	Proceed to Next Task	If enabled. Updated at ingestion
.upon_reject	Incident/Event Attribute	Upon Reject	.sys_create_d_on	Cancel all future Tasks	If enabled. Updated at ingestion
.urgency	Incident/Event Attribute	Urgency	.sys_create_d_on	Low	If enabled. Updated at ingestion

ServiceNow Security Cases

The ServiceNow Security Cases feed ingests cases from ServiceNow's Threat Intelligence module into ThreatQ.

Included with each incident will be the following:

- Related Observables
- Related Adversaries
- Work Notes, Comments, & Automated Activities

GET https://{sub-domain}.service-now.com/api/now/v1/table/sn_ti_case

Sample Response:

```
{
  "result": [
    {
      "parent": "",
      "made_sla": "true",
      "last_seen": "2022-08-31 13:20:42",
      "watch_list": "",
      "rating": "High",
      "upon_reject": "Cancel all future Tasks",
      "sys_updated_on": "2022-08-31 13:20:42",
      "task_effective_number": "SECC0001002",
      "approval_history": "",
      "skills": "",
      "number": "SECC0001002",
      "sys_updated_by": "admin",
      "opened_by": {
        "display_value": "System Administrator",
        "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/6816f79cc0a8016401c5a33be04be441"
      },
      "user_input": "",
      "sys_created_on": "2022-08-31 13:19:31",
      "sys_domain": {
        "display_value": "global",
        "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user_group/global"
      },
      "state": "Open",
      "route_reason": "",
      "sys_created_by": "admin",
      "knowledge": "false",
      "order": "",
      "closed_at": "",
      "cmdb_ci": "",
      "delivery_plan": "",
      "contract": "",
      "impact": "3 - Low",
      "active": "true",
      "work_notes_list": "",
      "business_service": "",
      "priority": "4 - Low",
      "sys_domain_path": "/",
      "time_worked": "",
      "expected_start": "",
      "opened_at": "2022-08-31 13:18:43",
      "business_duration": "",
      "group_list": ""
    }
  ]
}
```

```

    "work_end": "",
    "approval_set": "",
    "work_notes": "",
    "security_tags": "",
    "universal_request": "",
    "short_description": "OpMurica",
    "correlation_display": "",
    "delivery_task": "",
    "work_start": "",
    "assignment_group": "",
    "additional_assignee_list": "",
    "description": "A case tracking OpMurica's progress",
    "calendar_duration": "",
    "close_notes": "",
    "service_offering": "",
    "sys_class_name": "Security Case",
    "closed_by": "",
    "follow_up": "",
    "sys_id": "cfab6edb47ad5110fbc4e357536d4310",
    "contact_type": null,
    "urgency": "3 - Low",
    "company": "",
    "reassignment_count": "0",
    "activity_due": "UNKNOWN",
    "assigned_to": "",
    "comments": "",
    "approval": "Not Yet Requested",
    "sla_due": "UNKNOWN",
    "comments_and_work_notes": "",
    "due_date": "",
    "sys_mod_count": "2",
    "case_type": "Campaign",
    "sys_tags": "",
    "escalation": "Normal",
    "upon_approval": "Proceed to Next Task",
    "correlation_id": "",
    "location": ""
  }
]
}

```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the result list. Additional mappings are handled by the [ServiceNow Observables](#), [Get Related Threat Actors](#), and [Get Related Intrusion Sets](#) feeds.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.number, .case_type, .short_description	Incident/Event Value	N/A	.sys_created_on	SECC0001001 \\ Campaign \\ OpMurica	N/A
.security_tags	Incident/Event Tag	N/A	N/A	TLP: RED	If enabled. Tags containing : are updated.
.description	Incident/Event Description	N/A	N/A	A case tracking OpMurica's...	Concatenated with other values.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.activity_due	Incident/Event Attribute	Activity Due	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.approval	Incident/Event Attribute	Approval Status	.sys_create_d_on	Not Yet Requested	If enabled. Updated at ingestion
.assigned_to.display_value	Incident/Event Attribute	Assigned To	.sys_create_d_on	John Doe	If enabled. Updated at ingestion
.assignment_group.display_value	Incident/Event Attribute	Assignment Group	.sys_create_d_on	Windows Security	If enabled. Updated at ingestion
.case_type	Incident/Event Attribute	Case Type	.sys_create_d_on	Campaign	If enabled. Updated at ingestion
.category	Incident/Event Attribute	Category	.sys_create_d_on	Unauthorized access	If enabled. Updated at ingestion
.close_notes	Incident/Event Attribute	Close Note	.sys_create_d_on	Solved	If enabled
.closed_at	Incident/Event Attribute	Closed At	.sys_create_d_on	N/A	If enabled
.closed_by.display_value	Incident/Event Attribute	Closed By	.sys_create_d_on	N/A	If enabled
.contact_type	Incident/Event Attribute	Contact Type	.sys_create_d_on	Phone	If enabled. Updated at ingestion
.sys_created_by	Incident/Event Attribute	Created By	.sys_create_d_on	si_admin	If enabled.
.escalation	Incident/Event Attribute	Escalation Status	.sys_create_d_on	Normal	If enabled. Updated at ingestion
.estimated_end	Incident/Event Attribute	Estimated End	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.expected_end	Incident/Event Attribute	Expected End	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.expected_start	Incident/Event Attribute	Expected Start	.sys_create_d_on	2022-09-10 10:19:36	If enabled. Updated at ingestion
.impact	Incident/Event Attribute	Impact	.sys_create_d_on	Low	If enabled. Updated at ingestion
.active	Incident/Event Attribute	Is Active	.sys_create_d_on	true	If enabled. Updated at ingestion
.location.display_value	Incident/Event Attribute	Location	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.opened_at	Incident/Event Attribute	Opened At	.sys_create_d_on	2022-08-09 06:34:13	If enabled. Updated at ingestion
.opened_by	Incident/Event Attribute	Opened By	.sys_create_d_on	System Administrator	If enabled. Updated at ingestion
.priority	Incident/Event Attribute	Priority	.sys_create_d_on	Low	If enabled. Updated at ingestion
.rating	Incident/Event Attribute	Rating	.sys_create_d_on	High	If enabled. Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.sys_id	Incident/Event Attribute	ServiceNow Link	.sys_created_on	N/A	If enabled. Concatenated with host. Updated at ingestion
.severity	Incident/Event Attribute	Severity	.sys_created_on	Medium	If enabled. Updated at ingestion
.state	Incident/Event Attribute	State	.sys_created_on	Open	If enabled. Updated at ingestion
.substate	Incident/Event Attribute	Substate	.sys_created_on	N/A	If enabled. Updated at ingestion
.number	Incident/Event Attribute	System Number	.sys_created_on	SECC0001001	If enabled. Updated at ingestion
.upon_approval	Incident/Event Attribute	Upon Approval	.sys_created_on	Proceed to Next Task	If enabled. Updated at ingestion
.upon_reject	Incident/Event Attribute	Upon Reject	.sys_created_on	Cancel all future Tasks	If enabled. Updated at ingestion
.urgency	Incident/Event Attribute	Urgency	.sys_created_on	Low	If enabled. Updated at ingestion

ServiceNow Security Incident Response Task

The ServiceNow Security Incident Response Task feed automatically ingests incident response tasks from ServiceNow's Security Incident Response module, into ThreatQ.

Included with each incident will be the following:

- Related Observables

GET https://{sub-domain}.service-now.com/api/now/v1/table/sn_si_task

Sample Response:

```
{
  "result": [
    {
      "parent": {
        "display_value": "SIR0000041",
        "link": "https://ven04020.service-now.com/api/now/table/task/c9877b53db647b009f7890b6db9619e8"
      },
      "window_end": "",
      "watch_list": "",
      "upon_reject": "Cancel all future Tasks",
      "sys_updated_on": "2019-04-07 01:23:03",
      "approval_history": "",
      "skills": "",
      "number": "SIT0000046",
      "previous_agent": "",
      "expected_travel_start": "",
      "state": "Closed Complete",
      "sys_created_by": "sirphishbox",
      "knowledge": "false",
      "order": "",
      "delivery_plan": "",
      "contract": "",
      "impact": "3 - Low",
      "active": "false",
      "work_notes_list": "",
      "priority": "4 - Low",
      "sys_domain_path": "/",
      "business_duration": "",
      "group_list": "",
      "approval_set": "",
      "universal_request": "",
      "template": "",
      "short_description": "Acknowledge User Submission and ask user if they interacted with the email",
      "acknowledged_on": "",
      "correlation_display": "",
      "delivery_task": "",
      "work_start": ""
    }
  ]
}
```

```

    "affected_user": "",
    "additional_assignee_list": "",
    "actual_travel_start": "",
    "estimated_travel_duration": "1 Hour",
    "assigned_vendor": "",
    "service_offering": "",
    "sys_class_name": "Security Incident Response Task",
    "closed_by": {
      "display_value": "Gwen Broaden",
      "link": "https://ven04020.service-now.com/api/now/table/sys_user/
340e7436db64f700db9b9875db9619ea"
    },
    "follow_up": "",
    "si_state": "Analysis",
    "estimated_end": "2019-04-07 01:40:25",
    "vendor_reference": "",
    "dispatched_on": "",
    "reassignment_count": "0",
    "outcome": null,
    "assigned_to": {
      "display_value": "Gwen Broaden",
      "link": "https://ven04020.service-now.com/api/now/table/sys_user/
340e7436db64f700db9b9875db9619ea"
    },
    "sla_due": "UNKNOWN",
    "comments_and_work_notes": "",
    "substate": "",
    "escalation": "Normal",
    "upon_approval": "Proceed to Next Task",
    "correlation_id": "",
    "asset": "",
    "made_sla": "true",
    "task_effective_number": "SIT0000046",
    "sys_updated_by": "gbroaden",
    "opened_by": {
      "display_value": "SIR Phisbox",
      "link": "https://ven04020.service-now.com/api/now/table/sys_user/
f5c6dd36dba4f700db9b9875db9619a5"
    },
    "user_input": "",
    "sys_created_on": "2019-04-07 00:40:25",
    "sys_domain": {
      "display_value": "global",
      "link": "https://ven04020.service-now.com/api/now/table/sys_user_group/
global"
    },
    "route_reason": "",
    "is_fixed_window": "false",
    "closed_at": "2019-04-07 01:23:03",
    "window_start": "",

```



```

    "business_service": "",
    "time_worked": "",
    "expected_start": "2019-04-07 00:40:25",
    "opened_at": "2019-04-07 00:40:25",
    "work_end": "2019-04-07 01:23:03",
    "outcome_type": null,
    "work_notes": "",
    "security_tags": "",
    "initiated_from": "",
    "assignment_group": {
      "display_value": "SIRT",
      "link": "https://ven04020.service-now.com/api/now/table/sys_user_group/
dea26263ff0331007a6dffffffffffff19"
    },
    "under_warranty": "false",
    "actual_travel_duration": "",
    "description": "Investigate hashes",
    "calendar_duration": "",
    "flow_context_id": "",
    "close_notes": "",
    "dispatch_group": "",
    "sys_id": "3187bb53db647b009f7890b6db9619bc",
    "contact_type": null,
    "urgency": "3 - Low",
    "secure_notes": "",
    "company": "",
    "activity_due": "UNKNOWN",
    "comments": "",
    "approval": "Not Yet Requested",
    "has_follow_on": "false",
    "due_date": "2019-04-07 00:40:25",
    "sys_mod_count": "2",
    "sys_tags": "Customer Service",
    "estimated_work_duration": "1 Hour",
    "routing_in_progress": "false",
    "location": "",
    "cloned_from": ""
  }
]
}

```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the `result` list. Additional mappings are handled by the [ServiceNow Observables](#) feed. If the **Ingest Parent Incident** configuration option is enabled, the value `.parent.link` is sent to **ServiceNow Get Object By Link** feed. The feed retrieves the parent incident that is processed the same as the current ingested incident.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.number, .short_description</code>	Incident/Event Value	N/A	<code>.sys_created_on</code>	SIT0000046 Single sirt with all objects	N/A
<code>.sys_tags</code>	Incident/Event Tag	N/A	N/A	Customer Service	If enabled. Tags containing : are updated.
<code>.description</code>	Incident/Event Description	N/A	N/A	Investigate hashes	Concatenated with other values.
<code>.activity_due</code>	Incident/Event Attribute	Activity Due	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.affected_user</code>	Incident/Event Attribute	Affected User	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.approval</code>	Incident/Event Attribute	Approval Status	<code>.sys_created_on</code>	Not Yet Requested	If enabled. Updated at ingestion
<code>.assigned_to.display_value</code>	Incident/Event Attribute	Assigned To	<code>.sys_created_on</code>	John Doe	If enabled. Updated at ingestion
<code>.assignment_group.display_value</code>	Incident/Event Attribute	Assignment Group	<code>.sys_created_on</code>	Windows Security	If enabled. Updated at ingestion
<code>.close_notes</code>	Incident/Event Attribute	Close Note	<code>.sys_created_on</code>	Solved	If enabled
<code>.closed_at</code>	Incident/Event Attribute	Closed At	<code>.sys_created_on</code>	N/A	If enabled
<code>.closed_by.display_value</code>	Incident/Event Attribute	Closed By	<code>.sys_created_on</code>	N/A	If enabled
<code>.contact_type</code>	Incident/Event Attribute	Contact Type	<code>.sys_created_on</code>	Phone	If enabled. Updated at ingestion
<code>.sys_created_by</code>	Incident/Event Attribute	Created By	<code>.sys_created_on</code>	si_admin	If enabled.
<code>.escalation</code>	Incident/Event Attribute	Escalation Status	<code>.sys_created_on</code>	Normal	If enabled. Updated at ingestion
<code>.estimated_end</code>	Incident/Event Attribute	Estimated End	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.expected_end</code>	Incident/Event Attribute	Expected End	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.expected_start</code>	Incident/Event Attribute	Expected Start	<code>.sys_created_on</code>	2022-09-10 10:19:36	If enabled. Updated at ingestion
<code>.hold_reason</code>	Incident/Event Attribute	Hold Reason	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.impact	Incident/Event Attribute	Impact	.sys_create_d_on	High	If enabled. Updated at ingestion
.active	Incident/Event Attribute	Is Active	.sys_create_d_on	true	If enabled. Updated at ingestion
.location.display_value	Incident/Event Attribute	Location	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.made_sla	Incident/Event Attribute	Made SLA	.sys_create_d_on	true	If enabled. Updated at ingestion
.opened_at	Incident/Event Attribute	Opened At	.sys_create_d_on	2022-08-09 06:34:13	If enabled. Updated at ingestion
.opened_by	Incident/Event Attribute	Opened By	.sys_create_d_on	System Administrator	If enabled. Updated at ingestion
.priority	Incident/Event Attribute	Priority	.sys_create_d_on	Critical	If enabled. Updated at ingestion
.sys_id	Incident/Event Attribute	ServiceNow Link	.sys_create_d_on	N/A	If enabled. Concatenated with host. Updated at ingestion
.severity	Incident/Event Attribute	Severity	.sys_create_d_on	Medium	If enabled. Updated at ingestion
.state	Incident/Event Attribute	State	.sys_create_d_on	Closed	If enabled. Updated at ingestion
.substate	Incident/Event Attribute	Substate	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.number	Incident/Event Attribute	System Number	.sys_create_d_on	SIT0000046	If enabled. Updated at ingestion
.upon_approval	Incident/Event Attribute	Upon Approval	.sys_create_d_on	Proceed to Next Task	If enabled. Updated at ingestion
.upon_reject	Incident/Event Attribute	Upon Reject	.sys_create_d_on	Cancel all future Tasks	If enabled. Updated at ingestion
.urgency	Incident/Event Attribute	Urgency	.sys_create_d_on	Low	If enabled. Updated at ingestion

ServiceNow Service Desk Incidents

The ServiceNow Security Incident Response Task feed automatically ingests service desk incidents from ServiceNow into ThreatQ.

Included with each incident will be the following:

- Related Observables

GET <https://{sub-domain}.service-now.com/api/now/v1/table/incident>

Sample Response:

```
{
  "result": [
    {
      "active": "false",
      "activity_due": "2016-12-12 17:26:36",
      "additional_assignee_list": "",
      "approval": "Not Yet Requested",
      "approval_history": "",
      "approval_set": "",
      "assigned_to": {
        "display_value": "David Loo",
        "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/5137153cc611227c000bbd1bd8cd2007"
      },
      "assignment_group": {
        "display_value": "Network",
        "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user_group/287ebd7da9fe198100f92cc8d1d2154e"
      },
      "business_duration": "8 Hours",
      "business_impact": "",
      "business_service": {
        "display_value": "Email",
        "link": "https://dev63597.service-now.com/api/now/v1/table/cmdb_ci_service/27d32778c0a8000b00db970eeaa60f16"
      },
      "business_stc": "28,800",
      "calendar_duration": "1 Day 4 Hours 23 Minutes",
      "calendar_stc": "102,197",
      "caller_id": {
        "display_value": "Joe Employee",
        "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/681ccaf9c0a8016400b98a06818d57c7"
      },
      "category": "Inquiry / Help",
      "cause": "",
      "caused_by": "",
      "child_incidents": "0",
      "close_code": "Solved (Permanently)",
    }
  ]
}
```

```

    "close_notes": "This incident is resolved.",
    "closed_at": "2016-12-13 18:46:44",
    "closed_by": {
      "display_value": "Joe Employee",
      "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/681ccaf9c0a8016400b98a06818d57c7"
    },
    "cmdb_ci": {
      "display_value": "Storage Area Network 001",
      "link": "https://dev63597.service-now.com/api/now/v1/table/cmdb_ci/109562a3c611227500a7b7ff98cc0dc7"
    },
    "comments": "2016-12-13 12:30:14 - Joe Employee (Additional comments)\nHi David, \nThat must be it. I was on phone calls at all three of those times and must not have had any activity on my computer. Please close this incident.\n\n2016-12-13 10:42:25 - David Loo (Additional comments)\nHi Joe,\nI've checked in network logs and you were timed out from the VPN at 9:25AM, 10:42AM and 2:28PM. These three times coincide with entries in the exchange server logs showing you lost connection at those same times. The VPN policy is to time out a connection if it hasn't been active in 30 minutes. Please ensure the next time you lose connectivity you are still connected to the VPN.\n\nI'm going to update this incident to resolved. Please let me know if you need any more assistance.\n\n2016-12-13 07:53:01 - Joe Employee (Additional comments)\nHi David,\nThank you! I use the corporate VPN and was also unable to connect to the email server at 9:30AM and 10:45AM.\n\n2016-12-13 06:43:17 - David Loo (Additional comments)\nHi Joe,\nMy name is David. I'll be assisting you with this incident. Can you confirm which VPN you have been using today? I also see you were having this issue at 2:30PM. Were there any other times you can recall you had issues connecting to the email?\n\n2016-12-12 16:56:57 - Beth Anglin (Additional comments)\nHi Joe, \nAs per discussion on call, Workaround has been provided and it has worked for you. I have verified with the Exchange team we haven't had an issue with the email server today. I'm going to assign this issue to the network team for further investigation.\n\n2016-12-12 12:43:50 - Joe Employee (Additional comments)\nHi Beth,\nYes, I'm connected to the VPN, although I've had to reconnect to it a couple of times. The last time I was unable to connect was 2:30PM.\n\n2016-12-12 10:52:42 - Beth Anglin (Additional comments)\nHi Joe, \nAre you connected to the VPN when you're having this issue? Can you identify a specific time you were unable to connect to email?\n\n2016-12-12 08:30:49 - Beth Anglin (Additional comments)\nHi Joe, \nMy name is Beth and I'll be assisting you with your issue.\n\n2016-12-12 07:19:57 - Joe Employee (Additional comments)\nI am unable to connect to the email server. It appears to be down.\n\n",
    "comments_and_work_notes": "2016-12-13 12:30:14 - Joe Employee (Additional comments)\nHi David, \nThat must be it. I was on phone calls at all three of those times and must not have had any activity on my computer. Please close this incident.\n\n2016-12-13 10:42:25 - David Loo (Additional comments)\nHi Joe,\nI've checked in network logs and you were timed out from the VPN at 9:25AM, 10:42AM and 2:28PM. These three times coincide with entries in the exchange server logs showing you lost connection at those same times. The VPN policy is to time out a connection if it hasn't been active in 30 minutes.

```

Please ensure the next time you lose connectivity you are still connected to the VPN.

I'm going to update this incident to resolved. Please let me know if you need any more assistance.

2016-12-13 07:53:01 - Joe Employee (Additional comments)

Hi David,

Thank you! I use the corporate VPN and was also unable to connect to the email server at 9:30AM and 10:45AM.

2016-12-13 06:43:17 - David Loo (Additional comments)

Hi Joe,

My name is David. I'll be assisting you with this incident. Can you confirm which VPN you have been using today? I also see you were having this issue at 2:30PM. Were there any other times you can recall you had issues connecting to the email?

2016-12-12 16:56:57 - Beth Anglin (Additional comments)

Hi Joe,

As per discussion on call, Workaround has been provided and it has worked for you. I have verified with the Exchange team we haven't had an issue with the email server today. I'm going to assign this issue to the network team for further investigation.

2016-12-12 16:56:57 - Beth Anglin (Work notes)

Updating priority as workaround for incident has been provided.

2016-12-12 12:43:50 - Joe Employee (Additional comments)

Hi Beth,

Yes, I'm connected to the VPN, although I've had to reconnect to it a couple of times. The last time I was unable to connect was 2:30PM.

2016-12-12 10:52:42 - Beth Anglin (Additional comments)

Hi Joe,

Are you connected to the VPN when you're having this issue? Can you identify a specific time you were unable to connect to email?

2016-12-12 09:57:00 - Beth Anglin (Work notes)

Increasing priority as this incident is affecting more number of users

2016-12-12 09:01:24 - Beth Anglin (Work notes)

Updating incident with correct Configuration item

2016-12-12 08:30:49 - Beth Anglin (Additional comments)

Hi Joe,

My name is Beth and I'll be assisting you with your issue.

2016-12-12 07:19:57 - Joe Employee (Additional comments)

I am unable to connect to the email server. It appears to be down.

```

    "company": {
      "display_value": "ACME North America",
      "link": "https://dev63597.service-now.com/api/now/v1/table/core_company/31bea3d53790200044e0bfc8bcbe5dec"
    },
    "contact_type": "Self-service",
    "contract": "",
    "correlation_display": "",
    "correlation_id": "",
    "delivery_plan": "",
    "delivery_task": "",
    "description": "I am unable to connect to the email server. It appears to be down.",
    "due_date": "",
    "escalation": "Normal",
    "expected_start": "",
    "follow_up": "",
    "group_list": "",
    "hold_reason": "",
    "impact": "2 - Medium",
    "incident_state": "Closed",
    "knowledge": "false",
    "location": "",
    "made_sla": "true",

```

```

    "notify": "Do Not Notify",
    "number": "INC0000060",
    "opened_at": "2016-12-12 07:19:57",
    "opened_by": {
      "display_value": "Joe Employee",
      "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/
681ccaf9c0a8016400b98a06818d57c7"
    },
    "order": "",
    "origin_id": "",
    "origin_table": "",
    "parent": "",
    "parent_incident": "",
    "priority": "3 - Moderate",
    "problem_id": "",
    "reassignment_count": "2",
    "reopen_count": "0",
    "reopened_by": "",
    "reopened_time": "",
    "resolved_at": "2016-12-13 13:43:14",
    "resolved_by": {
      "display_value": "David Loo",
      "link": "https://dev63597.service-now.com/api/now/v1/table/sys_user/
5137153cc611227c000bbd1bd8cd2007"
    },
    "rfc": "",
    "route_reason": "",
    "service_offering": "",
    "severity": "3 - Low",
    "short_description": "Unable to connect to email",
    "skills": "",
    "sla_due": "UNKNOWN",
    "state": "Closed",
    "subcategory": "Email",
    "sys_class_name": "Incident",
    "sys_created_by": "employee",
    "sys_created_on": "2016-12-12 07:19:57",
    "sys_domain": {
      "display_value": "global",
      "link": "https://dev63597.service-now.com/api/now/v1/table/
sys_user_group/global"
    },
    "sys_domain_path": "/",
    "sys_id": "1c741bd70b2322007518478d83673af3",
    "sys_mod_count": "15",
    "sys_tags": "Windows",
    "sys_updated_by": "employee",
    "sys_updated_on": "2016-12-13 18:46:44",
    "task_effective_number": "INC0000060",
    "time_worked": "",

```

```

    "universal_request": "",
    "upon_approval": "Proceed to Next Task",
    "upon_reject": "Cancel all future Tasks",
    "urgency": "2 - Medium",
    "user_input": "",
    "watch_list": "",
    "work_end": "",
    "work_notes": "2016-12-12 16:56:57 - Beth Anglin (Work notes)\nUpdating
priority as workaround for incident has been provided.\n\n2016-12-12 09:57:00 -
Beth Anglin (Work notes)\nIncreasing priority as this incident is affecting
more number of users\n\n2016-12-12 09:01:24 - Beth Anglin (Work notes)
\nUpdating incident with correct Configuration item\n\n",
    "work_notes_list": "",
    "work_start": ""
  }
]
}

```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the result list. Additional mappings are handled by the [ServiceNow Observables](#) feed. If Ingest Parent Incident option is enabled the value `.parent_incident.link` is sent to **ServiceNow Get Object By Link** supplemental feed. The feed retrieves the parent incident that is processed the same as the current ingested incident.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.number,</code> <code>.short_description</code>	Incident/Event Value	N/A	<code>.sys_created_on</code>	INC0000060 Unable to connect to email	N/A
<code>.sys_tags</code>	Incident/Event Tag	N/A	N/A	Windows	If enabled. Tags containing : are updated.
<code>.description</code>	Incident/Event Description	N/A	N/A	I am unable to connect to...	Concatenated with other values.
<code>.activity_due</code>	Incident/Event Attribute	Activity Due	<code>.sys_created_on</code>	N/A	If enabled. Updated at ingestion
<code>.approval</code>	Incident/Event Attribute	Approval Status	<code>.sys_created_on</code>	Not Yet Requested	If enabled. Updated at ingestion
<code>.assigned_to.display_value</code>	Incident/Event Attribute	Assigned To	<code>.sys_created_on</code>	John Doe	If enabled. Updated at ingestion
<code>.assignment_group.display_value</code>	Incident/Event Attribute	Assignment Group	<code>.sys_created_on</code>	Windows Security	If enabled. Updated at ingestion
<code>.caller_id.display_value</code>	Incident/Event Attribute	Caller	<code>.sys_created_on</code>	Joe Doe	If enabled. Updated at ingestion
<code>.category</code>	Incident/Event Attribute	Category	<code>.sys_created_on</code>	Unauthorized access	If enabled. Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.close_code	Incident/Event Attribute	Close Code	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.close_notes	Incident/Event Attribute	Close Note	.sys_create_d_on	Solved	If enabled
.closed_at	Incident/Event Attribute	Closed At	.sys_create_d_on	N/A	If enabled
.closed_by.display_value	Incident/Event Attribute	Closed By	.sys_create_d_on	N/A	If enabled
.contact_type	Incident/Event Attribute	Contact Type	.sys_create_d_on	Phone	If enabled. Updated at ingestion
.sys_created_by	Incident/Event Attribute	Created By	.sys_create_d_on	si_admin	If enabled.
.escalation	Incident/Event Attribute	Escalation Status	.sys_create_d_on	Normal	If enabled. Updated at ingestion
.expected_start	Incident/Event Attribute	Expected Start	.sys_create_d_on	2022-09-10 10:19:36	If enabled. Updated at ingestion
.hold_reason	Incident/Event Attribute	Hold Reason	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.impact	Incident/Event Attribute	Impact	.sys_create_d_on	High	If enabled. Updated at ingestion
.active	Incident/Event Attribute	Is Active	.sys_create_d_on	true	If enabled. Updated at ingestion
.location.display_value	Incident/Event Attribute	Location	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.opened_at	Incident/Event Attribute	Opened At	.sys_create_d_on	2022-08-09 06:34:13	If enabled. Updated at ingestion
.opened_by	Incident/Event Attribute	Opened By	.sys_create_d_on	System Administrator	If enabled. Updated at ingestion
.priority	Incident/Event Attribute	Priority	.sys_create_d_on	Critical	If enabled. Updated at ingestion
.sys_id	Incident/Event Attribute	ServiceNow Link	.sys_create_d_on	N/A	If enabled. Concatenated with host. Updated at ingestion
.severity	Incident/Event Attribute	Severity	.sys_create_d_on	Medium	If enabled. Updated at ingestion
.state	Incident/Event Attribute	State	.sys_create_d_on	Closed	If enabled. Updated at ingestion
.subcategory	Incident/Event Attribute	Subcategory	.sys_create_d_on	N/A	If enabled. Updated at ingestion
.number	Incident/Event Attribute	System Number	.sys_create_d_on	INC0000060	If enabled. Updated at ingestion
.upon_approval	Incident/Event Attribute	Upon Approval	.sys_create_d_on	Proceed to Next Task	If enabled. Updated at ingestion
.upon_reject	Incident/Event Attribute	Upon Reject	.sys_create_d_on	Cancel all future Tasks	If enabled. Updated at ingestion

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.urgency	Incident/Event Attribute	Urgency	.sys_created_on	Low	If enabled. Updated at ingestion



Additional mappings are handled by the ServiceNow Observables feed. If Ingest Parent Incident option is enabled the value .parent_incident.link is sent to ServiceNow Get Object By Link feed. The feed retrieves the parent incident that is processed the same as the current ingested incident.

ServiceNow Observables

The ServiceNow Observables feed automatically ingests observables from ServiceNow's Threat Intelligence module, into ThreatQ. The observables are ingested as indicators.

GET https://{sub-domain}.service-now.com/api/now/v1/table/sn_ti_observable

Sample Response:

```
{
  "result": [
    {
      "negation": "false",
      "mitre_tactic": "",
      "notes": "",
      "malicious_attachment": "",
      "sys_updated_on": "2024-06-07 00:11:09",
      "type": {
        "display_value": "Domain name",
        "link": "https://ven04020.service-now.com/api/now/table/sn_ti_observable_type/555d47809f81120035c6786f957fcf72"
      },
      "operator": null,
      "mitre_group": "",
      "sys_id": "017aa60b1b6e4e10d85e2f8a234bcb5f",
      "sys_updated_by": "admin",
      "sys_created_on": "2024-06-07 00:11:08",
      "sys_domain": {
        "display_value": "global",
        "link": "https://ven04020.service-now.com/api/now/table/sys_user_group/global"
      },
      "value": "telkomsacomininginbox.weebly.com",
      "sys_created_by": "admin",
      "mitre_malware": "",
      "finding_expiry_time": "",
      "sys_mod_count": "1",
      "is_composition": "false",
      "finding": "Malicious",
      "sys_tags": "",
      "mitre_data_source": "",
      "mitre_technique": "",
      "mitre_information": "",
      "sighting_count": "1",
      "mitre_platform": "",
      "location": "US",
      "mitre_tool": "",
      "security_tags": "Block from sharing, TLP: GREEN"
    }
  ]
}
```

```
]
}
```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the result list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.result[].value</code>	Indicator Value	<code>.result[].value.type.display_value</code>	<code>.sys_created_on</code>	telkomsacominginbox.weebly.com	See mapping table ServiceNow Observables Mapping
<code>.result[].notes</code>	Indicator Description	N/A	N/A	N/A	N/A
<code>.result[].negation</code>	Indicator Attribute	ServiceNow Negation	<code>.sys_created_on</code>	false	Updated at ingestion
<code>.result[].is_composition</code>	Indicator Attribute	ServiceNow Is Composition	<code>.sys_created_on</code>	false	Updated at ingestion
<code>.result[].finding</code>	Indicator Attribute	ServiceNow Finding	<code>.sys_created_on</code>	Malicious	Updated at ingestion
<code>.result[].location</code>	Indicator Attribute	ServiceNow Location	<code>.sys_created_on</code>	US	Updated at ingestion
<code>.result[].sighting_count</code>	Indicator Attribute	ServiceNow Sighting Count	<code>.sys_created_on</code>	1	Updated at ingestion
<code>.result[].sys_id</code>	Indicator Attribute	ServiceNow Link	<code>.sys_created_on</code>	https://{sub-domain}.service-now.com/now/nav/ui/classic/params/target/sn_ti_observable.do%3Fsys_id%3D{sys_id}	Updated at ingestion
<code>.result[].security_tags</code>	Indicator Tags	N/A	N/A	Block from sharing	Tags containing : are updated.

ServiceNow Observable Type to ThreatQ Indicator Type

The following table displays the ServiceNow Observable to ThreatQ Indicator type mapping.

SERVICENOW OBSERVABLE TYPE	THREATQ INDICATOR TYPE
unknown	String
e-mail	Email Address
SHA512	SHA-512
SHA160	SHA-1
FILEPATH	File Path
e-subject	Email Subject
cidr	CIDR Block
SHA384	SHA-384
FQDN	FQDN
ipv4-addr	IP Address
MUTEX	Mutex
asn	ASN
ipv6-addr	IPv6 Address
HOST	FQDN
mac	MAC Address

SERVICENOW OBSERVABLE TYPE	THREATQ INDICATOR TYPE
username	Username
SHA256	SHA-256
MD5	MD5
CVEID	CVE
URL	URL
URI	URL Path
TLD	FQDN
IP address (V4)	IP Address
Email address	Email address
SHA512 hash	SHA-512
File path	File path
Filename	Filename
CIDR rule	CIDR Block
SHA1 hash	SHA-1
Registry key	Registry key
Domain name	FQDN
MUTEX name	Mutex

SERVICENOW OBSERVABLE TYPE	THREATQ INDICATOR TYPE
SHA256 hash	SHA-256
MD5 hash	MD5
CVE number	CVE
Top-level domain name	FQDN
Unknown	String

Get Related Observables Supplemental

This supplemental feed fetches the observables related to a given ticket (task). This feed is called by any of the feeds: ServiceNow Security Incidents, ServiceNow Security Cases, ServiceNow Service Desk incidents, ServiceNow Security Incident Response Task if **Observables** is enabled in **Fetch Relationships** user configuration.

GET `https://{sub-domain}.service-now.com/api/now/v1/table/sn_ti_m2m_task_observable`

Sample Request Parameters:

```
{
  "sysparm_query": "task.number={task_effective_number}"
}
```

Sample Response:

```
{
  "result": [
    {
      "sys_id": "f23309f887f206103e9eeb1e3fbb35c2",
      "sys_updated_by": "admin",
      "task": {
        "link": "https://ven04020.service-now.com/api/now/table/task/
ac12c3591b0886507faea8a0604bcb4f",
        "value": "ac12c3591b0886507faea8a0604bcb4f"
      },
      "sys_created_on": "2024-06-12 10:09:32",
      "sys_domain": {
        "link": "https://ven04020.service-now.com/api/now/table/sys_user_group/global",
        "value": "global"
      },
      "context": "",
      "observable": {
        "link": "https://ven04020.service-now.com/api/now/table/sn_ti_observable/
ee0b6a8b1b6e4e10d85e2f8a234bcbde",
        "value": "ee0b6a8b1b6e4e10d85e2f8a234bcbde"
      },
      "sys_mod_count": "0",
      "sys_updated_on": "2024-06-12 10:09:32",
      "sys_tags": "",
      "lookup_requested": "false",
      "sys_created_by": "admin"
    }
  ]
}
```

There is no default mapping for this Feed. The Feed sends `.result.observable.link` them to [ServiceNow Get Object By Link](#) feed to get more information about the observable.

Get Object By Link Supplemental

The ServiceNow Get Object by Link supplemental feed fetches objects from ServiceNow using the link received as parameter.

```
GET https://{sub-domain}.service-now.com/api/now/table/sn_ti_observable/  
{observable_sys_id}
```

```
GET https://{sub-domain}.service-now.com/api/now/table/sn_si_incident/  
{si_incident_id}
```

```
GET https://{sub-domain}.service-now.com/api/now/table/sn_ti_case/{case_sys_id}
```

```
GET https://{sub-domain}.service-now.com/api/now/table/incident/  
{incident_sys_id}
```



There is no default mapping for this feed. The responses are the same as presented in the primary feeds using the same table.

Get Related Threat Actors Supplemental

The Get Related Threat Actors supplemental feed fetches the threat actors related to a given ticket (task).

GET https://{sub-domain}.service-now.com/api/now/v1/table/sn_ti_m2m_task_threat_actor

Sample Response:

```
{
  "result": [
    {
      "threat_actor.name": "Blackbyte Group"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the result list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.threat_actor.name	Adversary Name	N/A	N/A	Blackbyte Group	N/A

Get Related Intrusion Sets Supplemental

The Get Related Intrusion Sets supplemental feed fetches the intrusion sets related to a given ticket (task).

GET https://{sub-domain}.service-now.com/api/now/v1/table/sn_ti_m2m_task_intrusion_set

Sample Response:

```
{
  "result": [
    {
      "intrusion_set.name": "APT1"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:



Mappings are based on each item within the result list.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.intrusion_set.name	Adversary Name	N/A	N/A	APT1	N/A

Get Journal Entries Supplemental

The Get Journal Entries supplemental feed fetches the work notes, comments, and automation activities for a given ticket (task).

GET https://{sub-domain}.service-now.com/api/now/table/sys_journal_field

Sample Response:

```
{
  "result": [
    {
      "sys_id": "21c274a11b69715081630ed6624bcbfe",
      "sys_created_on": "2023-09-27 10:23:25",
      "name": "sn_si_incident",
      "element_id": "11c2b0a11b69715081630ed6624bcbb3",
      "sys_tags": "",
      "value": "Risk score changed from Empty to 40 due to change in business impact, priority, severity, risk score override",
      "sys_created_by": "admin",
      "element": "automation_activity"
    },
    {
      "sys_id": "8485978c1b31711044e321b3b24bcbe7",
      "sys_created_on": "2023-10-05 16:39:12",
      "name": "sn_si_incident",
      "element_id": "11c2b0a11b69715081630ed6624bcbb3",
      "sys_tags": "",
      "value": "ThreatQ Link: https://10.114.0.56/events/222/details",
      "sys_created_by": "admin",
      "element": "work_notes"
    }
  ]
}
```



Results are mapped to various sections of a ThreatQ Object's description.

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

ServiceNow Security Incidents

METRIC	RESULT
Run Time	1 minute
Adversaries	9
Attack Patterns	2
Incidents	25
Incident Attributes	426
Indicators	63
Indicator Attributes	29
Malware	15
Tools	4

ServiceNow Security Cases

METRIC	RESULT
Run Time	1 minute
Adversaries	3
Incidents	1
Incident Attributes	10
Indicators	4

ServiceNow Security Incident Response Task

METRIC	RESULT
Run Time	1 minute
Incidents	43
Incident Attributes	260
Indicators	32
Indicator Attributes	160

ServiceNow Service Desk Incidents

METRIC	RESULT
Run Time	1 minute
Incidents	62
Incident Attributes	496
Indicators	37
Indicator Attributes	185

ServiceNow Observables

METRIC	RESULT
Run Time	1 minute
Indicators	106
Indicator Attributes	530

Change Log

- **Version 2.0.0**
 - Added the following feeds:
 - ServiceNow Security Incident Response Task
 - ServiceNow Service Desk Incidents
 - ServiceNow Observables
 - The ServiceNow Security Incidents and Security Cases feeds will now ingest additional incident, indicator, and event attributes.
 - Updated the handling of tags that use the : character (**Example:** TLP:Green). If a ThreatQ object has a tag with the : character, the tag is deleted. If the object in ServiceNow has the same tag, the tag will be added back to the object. In the event that the ServiceNow object has different value for the tag, that value will be added as a new tag.
- **Version 1.1.0**
 - Added new configuration parameter: **Description Context**. This allows you to select context to include in each Incident's description. Options include Ticket Metadata, Ticket Description, and Closure Information.
 - Added improved description formatting when handling a JSON string description.
 - MITRE options for the Security Incidents feed are now disabled by default.
- **Version 1.0.1**
 - Added Unicode fixes.
 - Added two new options for the Fetch Relationships configuration parameter. Options now include Observable, Threat Actors, and Intrusion Sets.
 - Updated default selections for the Related Observable Type Filter parameters.
- **Version 1.0.0**
 - Initial release