ThreatQuotient

ServiceNow CDF User Guide

Version 1.0.1

November 20, 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

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.

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	1.0.1
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.

The integration ingests the following system objects:

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

Prerequisites

The ServiceNow CDF requires the **ServiceNow Security Incidents plugin** be installed in your ServiceNow instance/environment. Failure to do so will result in the integration not ingesting alerts.

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:

General 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. ⚠ This account should have the appropriate permissions to access the ServiceNow API.
ServiceNow Password	The password associated with the username above.
Date Field	Select the date field to use to filter results from ServiceNow. Options include: ◦ Created At ◦ Updated At (default)

PARAMETER	DESCRIPTION
	The **Updated At** option may overwrite existing tickets in ThreatQ based on the current ServiceNow context for a given incident.
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.
Related Observable Type Filter	Select the observable type to ingest from Related Observables. Options include: ◦ 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
Fetch Journal Entries	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. Enabling this will add +1 API calls per incident.
Parse Journal Entries for Indicators	Select the fields to parse for Indicators from the journal entries. This includes work notes, comments, and other automation activities. Options include: ◦ Work Notes ◦ Comments ◦ Automation Activities

PARAMETER	DESCRIPTION
Parse Indicator Types	Select the indicator types you would like to automatically parse from the content. Option include: ◦ CVE ◦ IP Address ◦ IPv6 Address ◦ CIDR Block ◦ FQDN ◦ URL ◦ MD5 ◦ SHA-1 ◦ SHA-256 ◦ SHA-512 ◦ Email Address ◦ Registry Key
Normalization Options	Select the normalization options you would like to use when parsing indicators from the content. Options include: ◦ Normalize Indicators (default) ◦ Derive FQDNs from URLs

Additional Parameters - Security Incidents

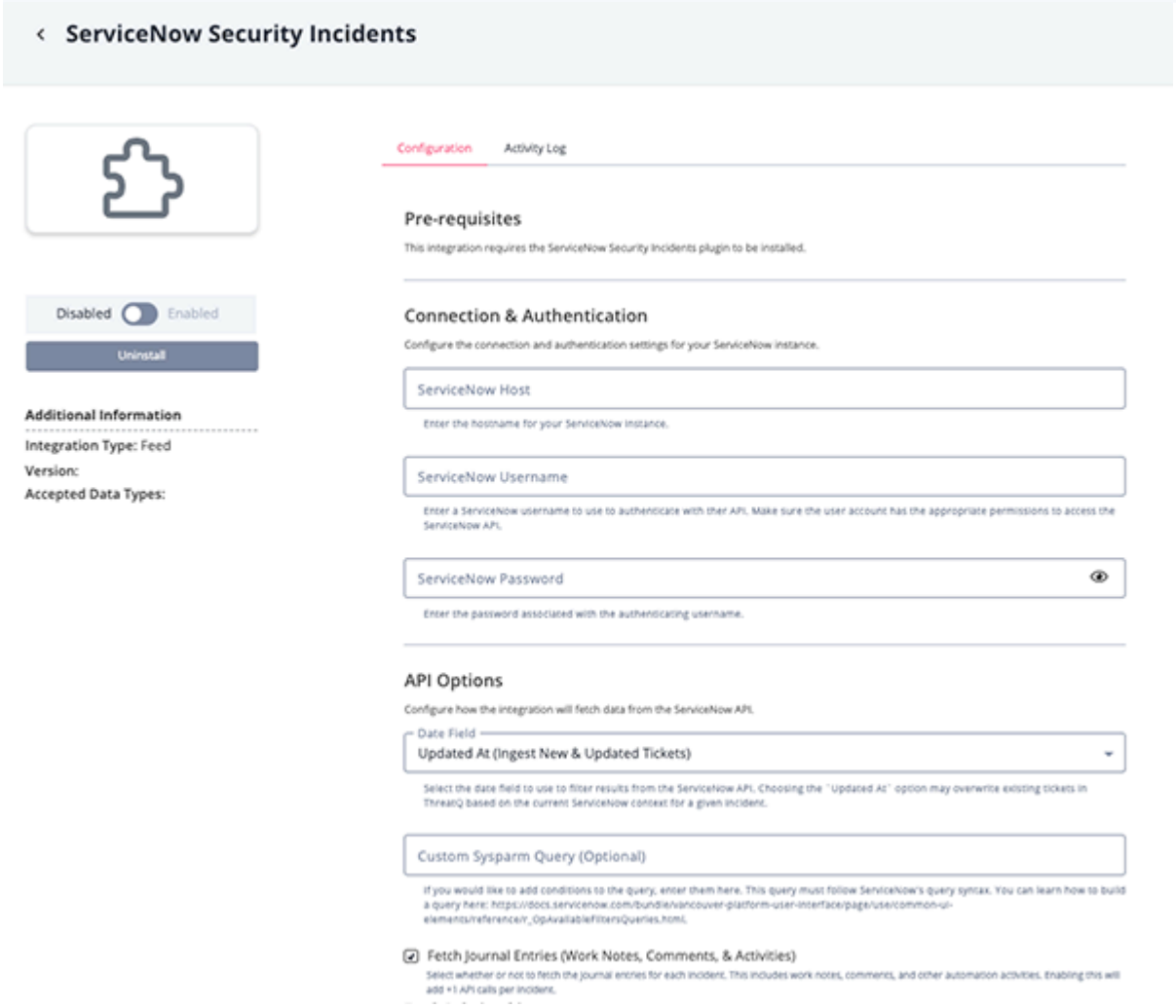
PARAMETER	DESCRIPTION
Fetch Relationships	Select the relationships to fetch for each case. Each selected relationship will add +1 API calls per case. Options include: ◦ Observables (default) ◦ Threat Actors (default) ◦ Intrusion Sets (default)
Incident Context	Select the incident context to bring in from ServiceNow. Options include: ◦ System Number (default) ◦ ServiceNow Link ◦ Tags (default) ◦ Is Active ◦ Activity Due ◦ Approval Status ◦ Assigned To (default) ◦ Close Code (default) ◦ Close Notes (default) ◦ Closed By (default) ◦ Confidence Score (default) ◦ Impact (default) ◦ Location ◦ Priority (default) ◦ Risk Score (default)

PARAMETER	DESCRIPTION
	◦ Assignment Group (default) ◦ Attack Vector (default) ◦ Business Criticality (default) ◦ Category (default) ◦ Subcategory (default) ◦ Closed At (default) ◦ Urgency (default) ◦ Escalation Status (default) ◦ State (default) ◦ Substate (default) ◦ Affected Platform (default)
Incident MITRE Context	Select the incident relationships to bring in from ServiceNow. Options include: ◦ MITRE ATT&CK Techniques (default) ◦ MITRE Tactics (default) ◦ Malware (default) ◦ Tools (default) ◦ Threat Actors (default)

Additional Parameters - Security Cases

PARAMETER	DESCRIPTION
Fetch Relationships	Select the relationships to fetch for each case. Each selected relationship will add +1 API calls per case. Options include: ◦ Observables (default) ◦ Threat Actors (default) ◦ Intrusion Sets (default)
Case Context	Select the case context to bring in from ServiceNow. Options include: ◦ System Number (default) ◦ ServiceNow Link ◦ Tags (default) ◦ Is Active ◦ Activity Due ◦ Approval Status ◦ Assigned To (default) ◦ Close Notes (default) ◦ Closed By (default) ◦ Impact (default) ◦ Location ◦ Priority (default) ◦ Urgency (default) ◦ Escalation Status (default)

PARAMETER	DESCRIPTION
	◦ Assignment Group (default) ◦ Closed At (default) ◦ Close Code (default) ◦ State (default) ◦ Rating (default)



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 Oborne",
        "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 (Keydnap),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/
9e1d0444ffa33100158bfffffffffffd"
      },
      "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 Oborne",
      "sys_id": "d8b6b953ff933100158bfffffffffff7f",
      "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/cmn_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 `Get Related Observables` supplemental feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.activity_due`	Incident Attribute	Activity Due	`.sys_created_on`	N/A	Attribute can be updated at runtime
`.mitre_platform`	Incident Attribute	Affected Platform	`.sys_created_on`	N/A	N/A
`.approval`	Incident Attribute	Approval Status	`.sys_created_on`	`Not Yet Requested`	Attribute can be updated at runtime
`.assigned_to.display_value`	Incident Attribute	Assigned To	`.sys_created_on`	`John Doe`	Attribute can be updated at runtime
`.assignment_group.display_value`	Incident Attribute	Assignment Group	`.sys_created_on`	`Windows Security`	N/A
`.attack_vector`	Incident Attribute	Attack Vector	`.sys_created_on`	`SQLi`	N/A
`.business_criticality`	Incident Attribute	Business Criticality	`.sys_created_on`	`Critical`	Attribute can be updated at runtime
`.category`	Incident Attribute	Category	`.sys_created_on`	`Unauthorized access`	N/A
`.close_notes`	Incident Attribute	Close Note	`.sys_created_on`	`Solved`	N/A
`.closed_at`	Incident Attribute	Closed At	`.sys_created_on`	N/A	N/A
`.closed_by.display_value`	Incident Attribute	Closed By	`.sys_created_on`	N/A	N/A
`.confidence_score`	Incident Attribute	Confidence Score	`.sys_created_on`	`55`	Attribute can be updated at runtime
`.escalation`	Incident Attribute	Escalation Status	`.sys_created_on`	`Normal`	Attribute can be updated at runtime
`.impact`	Incident Attribute	Impact	`.sys_created_on`	`High`	Attribute can be updated at runtime
`.active`	Incident Attribute	Is Active	`.sys_created_on`	`true`	Attribute can be updated at runtime
`.location.display_value`	Incident Attribute	Location	`.sys_created_on`	N/A	N/A
`.number`, `.short_description`	Incident Value	N/A	`.sys_created_on`	N/A	N/A
`.priority`	Incident Attribute	Priority	`.sys_created_on`	`Critical`	Attribute can be updated at runtime
`.risk_score`	Incident Attribute	Risk Score	`.sys_created_on`	`40`	Attribute can be updated at runtime

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.sys_id`	Incident Attribute	ServiceNow Link	`.sys_created_on`	N/A	Concatenated with host
`.severity`	Incident Attribute	Severity	`.sys_created_on`	`Medium`	Attribute can be updated at runtime
`.state`	Incident Attribute	State	`.sys_created_on`	`Closed`	Attribute can be updated at runtime
`.subcategory`	Incident Attribute	Subcategory	`.sys_created_on`	N/A	N/A
`.substate`	Incident Attribute	Substate	`.sys_created_on`	N/A	Attribute can be updated at runtime
`.tactic`	Incident Attribute	Tactic	`.sys_created_on`	`Reconnaissance`	N/A
`.urgency`	Incident Attribute	Urgency	`.sys_created_on`	`Low`	Attribute can be updated at runtime

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 Get Related Observables, Get Related Threat Actors, and Get Related Intrusion Sets supplemental feeds.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.number`, `.case_type`, `.short_description`	Incident Value	N/A	`.sys_created_on`	N/A	N/A
`.number`	Incident Attribute	System Number	`.sys_created_on`	`SECC0001001`	N/A
`.sys_id`	Incident Attribute	ServiceNow Link	`.sys_created_on`	N/A	Concatenated with ServiceNow host
`.active`	Incident Attribute	Is Active	`.sys_created_on`	`true`	Attribute can be updated at runtime
`.activity_due`	Incident Attribute	Activity Due	`.sys_created_on`	N/A	Attribute can be updated at runtime
`.approval`	Incident Attribute	Approval Status	`.sys_created_on`	`Not Yet Requested`	Attribute can be updated at runtime
`.assigned_to.display_value`	Incident Attribute	Assigned To	`.sys_created_on`	N/A	Attribute can be updated at runtime
`.assignment_group.display_value`	Incident Attribute	Assignment Group	`.sys_created_on`	N/A	Attribute can be updated at runtime
`.closed_at`	Incident Attribute	Closed At	`.sys_created_on`	N/A	N/A
`.close_notes`	Incident Attribute	Close Note	`.sys_created_on`	N/A	N/A
`.closed_by.display_value`	Incident Attribute	Closed By	`.sys_created_on`	N/A	N/A
`.impact`	Incident Attribute	Impact	`.sys_created_on`	`Low`	Attribute can be updated at runtime
`.location.display_value`	Incident Attribute	Location	`.sys_created_on`	N/A	N/A
`.priority`	Incident Attribute	Priority	`.sys_created_on`	`Low`	Attribute can be updated at runtime
`.urgency`	Incident Attribute	Urgency	`.sys_created_on`	`Low`	Attribute can be updated at runtime
`.escalation`	Incident Attribute	Escalation	`.sys_created_on`	`Normal`	Attribute can be updated at runtime
`.state`	Incident Attribute	State	`.sys_created_on`	`Open`	Attribute can be updated at runtime
`.rating`	Incident Attribute	Rating	`.sys_created_on`	`High`	Attribute can be updated at runtime

Get Related Observables Supplemental

The Get Related Observables supplemental feed fetches the observables related to a given ticket (task).

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

Sample Response:

```
{
  "result": [
    {
      "observable.value": "95.112.60.195",
      "observable.type.value": "ipv4-addr"
    },
    {
      "observable.value": "57.54.59.56",
      "observable.type.value": "ipv4-addr"
    }
  ]
}
```

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
`.observable.value`	Indicator Value	`.observable.type`	N/A	N/A	Type is mapped to the ThreatQ type

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

Change Log

- **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