ThreatQuotient

A Securonix Company

Samdesk CDF

Version 1.0.0

August 17, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Samdesk CDF integration enables ThreatQ to ingest alerts and event intelligence from Samdesk Search Streams via the Samdesk API. It transforms Samdesk data, including event details, locations, tags, updates, and proximity information, into structured ThreatQ Events and Event Attributes, providing additional real-world context for threat intelligence workflows.

The integration provides the following feed:

- **Samdesk Alerts** - ingests alert and event data from configured Samdesk Search Streams into ThreatQ, including event details, locations, tags, updates, and proximity information.

The integration ingests event and event attributes into the ThreatQ platform.

Prerequisites

The following is required to install and run the integration:

- A Samdesk API Key
- A Samdesk Search Stream ID

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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.

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:

PARAMETER	DESCRIPTION
API Key	Enter the Samdesk API key used to authenticate requests to the Samdesk API.
Stream IDs	Enter one or more Samdesk Search Stream IDs to retrieve alerts from. Specify one Stream ID per line.
Page Size	Specify the maximum number of alerts to retrieve per API request.
Include Dismissed Alerts	Enable this parameter to include dismissed alerts in the data retrieved from Samdesk.
Dashboard-only Updates	Enable this parameter to restrict retrieved results to updates designated for the Samdesk dashboard.
Include Locality Fields	Enable this parameter to request locality-related fields from the Samdesk API.

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

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

Samdesk Alerts

The Samdesk Alerts feed ingests alert and event data from configured Samdesk Search Streams into ThreatQ, including event details, locations, tags, updates, and proximity information.

```
GET https://api.samdesk.io/1/search_streams/{search_stream_id}/alerts
```

Sample Response:

```
{
  "count": 2,
  "data": [
    {
      "id": "alert_001",
      "alert_type": "incident",
      "alert_text": "Multi-vehicle collision reported on Highway 401
near Toronto.",
      "created": 1783177200000,
      "url": "https://app.samdesk.io/search_streams/stream_001/
alerts/alert_001",
      "event": {
        "id": "event_001",
        "headline": "Highway 401 collision near Toronto",
        "summary_text": "Emergency services are responding to a
multi-vehicle collision affecting eastbound lanes.",
        "time": 1783176840000,
        "severity": "high",
        "types": ["traffic", "transportation"],
        "tags": ["collision", "road-closure", "toronto"],
        "locations": [
          { "text": "Highway 401", "lat": 43.6532, "lon": -79.3832 },
          { "text": "Toronto, Ontario, Canada", "lat": 43.65107,
"lon": -79.347015 }
        ],
        "proximity_matches": [
          { "asset_type": "location", "name": "Toronto Pearson
International Airport", "distance": 18700 },
          { "asset_type": "location", "name": "Downtown Toronto",
"distance": 9200 }
```

```
        ],
        "updates": [
          {
            "time": 1783176960000,
            "type": "note",
            "text": "Two eastbound lanes remain blocked while cleanup
is in progress."
          }
        ]
      }
    }
  ],
  "pagination": {
    "after": 1783179000000,
    "before": 1783177200000
  }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].id	Event.Attribute	Alert ID	.data[].created	alert_001	Event identifier
.data[].alert_text	Event.description	Description	.data[].created	Multi-vehicle collision reported...	Alert summary text
.data[].event.headline	Event.value	Title	.data[].event.time	Highway 401 collision near Toronto	Event title
.data[].event.summary_text	Event.description	Description	.data[].event.time	Emergency services are responding...	Contextual summary
.data[].event.tags[]	Event.Tag	Tag	N/A	collision	Event tags
.data[].event.types[]	Event.Attribute	Type	N/A	traffic	Event types
.data[].event.locations[]	Event.Attribute	Location	N/A	Toronto, Ontario, Canada	Location contex
.data[].event.updates[]	Event.description	Description	N/A	Two eastbound lanes remain blocked...	Update context
.data[].event.proximity_matches[]	Event.Attribute	Proximity Matches	N/A	Toronto Pearson International Airport	Proximity enrichment
.data[].url	Event.Attribute	Dashboard Link	.data[].created	https://app.samdesk.io/...	Source link

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.

METRIC	RESULT
Run Time	2 minutes
Event	2
Event Attributes	22

Change Log

- **Version 1.0.0**
  - Initial release