ThreatQuotient

Splunk Assets CDF

Version 1.0.0

January 28, 2025

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	1.0.0
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

The Splunk Assets CDF integration queries Splunk to ingest assets and identities related to sighting events. If sighting events were already ingested into ThreatQ using ThreatQuotient App for Splunk then the assets and identities will be related to them.

The integration provides the following feed:

- **Splunk Assets -** ingests assets and identities related to sighting events.

The integration ingests the following object types:

- Assets
- Events
- Identities
- Indicators

Prerequisites

The integration requires the following:

- A Splunk instance
- The following Splunk instance details:
  - Splunk Host
  - Splunk API Port
  - Splunk Username
  - Splunk Password
- A Splunk Search Report (Saved Search) titled: `SOCThreatQgetassets`

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
6. Select the individual feeds to install, when prompted and click **Install**.

    > 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(s) 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.

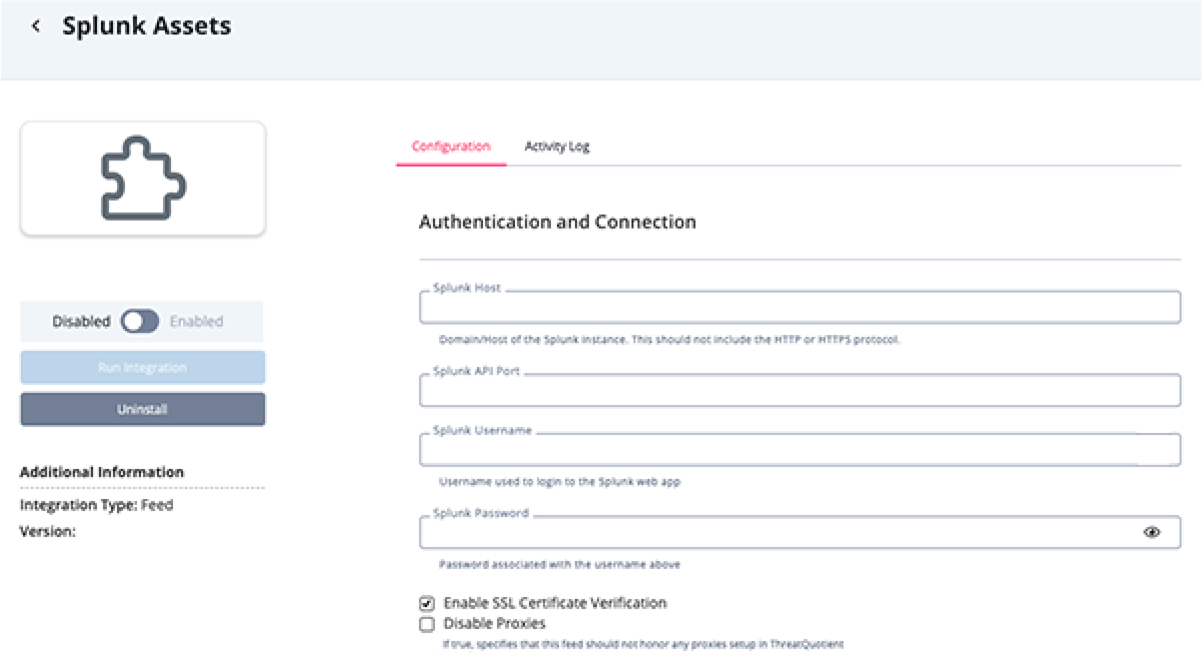
To configure the integration:

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
Splunk Host	Enter the domain/host of your Splunk instance.
Splunk API Port	Enter the port number of the Splunk API.
Splunk Username	Enter the username used to log into the Splunk web application.
Splunk Password	Enter the password associated with the username above.
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



Splunk Assets

Additional Information

Integration Type: Feed

Version:

Authentication and Connection

Splunk Host

Domain/Host of the Splunk instance. This should not include the HTTP or HTTPS protocol.

Splunk API Port

Splunk Username

Username used to login to the Splunk web app

Splunk Password

Password associated with the username above

☑ Enable SSL Certificate Verification

□ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

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

Splunk Assets

The Splunk Assets feed retrieves the search results from `SOCThreatQgetassets` Splunk report that were created after the feed start run time.

If a result contains the field `affected_asset` then a new asset is created using the value of this field.

If a result contains the field `affected_user` then a new identity is created using the value of this field.

If a result contains the field `indicator` then the integration gets all the ThreatQ Events of type `Sighting` that were created after feed start run time, and contain the value of the field `indicator`. It also gets the ThreatQ Indicator equal to the value of this field. The new asset and identity will be related to the exiting event and indicator in case they exist.

`GET https://{{SPLUNK_HOST}}:{{SPLUNK_API_PORT}}/services/search/v2/jobs/export`

Sample Request Parameters:

```
{
  "search": "savedsearch \"SOCThreatQgetassets\" | table *",
  "output_mode": "json",
  "earliest_time": "1735813371",
  "latest_time": "now"
}
```

Sample Response:

```
{
  "preview": false,
  "offset": 0,
  "result": {
    "affected_asset": "splunk1.threatq.com",
    "affected_user": "trent21identify",
    "asset_city": "new york",
    "asset_country": "united states",
    "asset_ip": "10.10.10.1",
    "asset_tag": "splunk1",
    "asset_timezone": "EEST",
    "date_hour": "0",
    "date_mday": "9",
    "date_minute": "0",
    "date_month": "january",
    "date_second": "0",
    "date_wday": "thursday",
    "date_year": "2025",
    "date_zone": "0",
    "host": "splunk",
    "identity_nick": "trent21",
    "identity_tag": "fc21",
    "identity_timezone": "EET",
    "identity_work_city": "madrid",
    "identity_work_country": "spain",
    "index": "main",
    "indicator": "cda48fc75952ad12d99e526d0b6bf70a",
    "linecount": "1",
    "punct": ",..,_,_,...,,,,,,,,,--_::._",
    "source": "splunk_input.csv",
    "sourcetype": "asssets_csv",
    "splunk_server": "splunk",
    "time": "2025-01-09 00:00:00.000 UTC",
    "_bkt": "main~4~73D94EC8-B29C-491E-BDD1-CF38C86CDE46",
    "_cd": "4:13",
    "_indextime": "1737538750",
    "_kv": "1",
    "_si": [
      "splunk",
      "main"
    ],
    "_sourcetype": "asssets_csv",
    "_subsecond": ".000",
    "_time": "2025-01-09 00:00:00.000 UTC"
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

> This mapping is based on each item within the `[].result` from the HTTP response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.affected_asset`	Asset.Value	N/A	N/A	`hostname1`	N/A
`.asset_tag`	Asset.Tag	N/A	N/A	`splunk1`	N/A
`.asset_city`	Asset.Attribute	Asset City	N/A	`New York`	Updatable. Title cased
`.asset_country`	Asset.Attribute	Asset Country	N/A	`United States`	Updatable. Title cased
`.asset_ip`	Asset.Attribute	IP Address	N/A	`10.10.10.1`	Updatable
`.asset_bunit`	Asset.Attribute	General Information	N/A	N/A	Updatable
`.asset_category`	Asset.Attribute	Asset Category	N/A	N/A	Updatable
`.asset_cim_entity_zone`	Asset.Attribute	CIM Entity Zone	N/A	N/A	Updatable
`.asset_lat`	Asset.Attribute	Asset Latitude	N/A	N/A	Updatable
`.asset_long`	Asset.Attribute	Asset Longitude	N/A	N/A	Updatable
`.asset_priority`	Asset.Attribute	Asset Criticality	N/A	N/A	Updatable
`.asset_dns`	Asset.Attribute	DNS Name	N/A	N/A	Updatable
`.asset_nt_host`	Asset.Attribute	NT Host	N/A	N/A	Updatable
`.asset_owner`	Asset.Attribute	Asset Owner	N/A	N/A	Updatable
`.asset_pci_domain`	Asset.Attribute	PCI Domain	N/A	N/A	Updatable
N/A	Asset.Attribute	Sighting Occurrences	N/A	1	Updatable. The number of recent ThreatQ Sighting Events where `.indicator` appears
`.affected_user`	Identity.Value	N/A	N/A	`trent`	N/A
`.identity_tag`	Identity.Tag	N/A	N/A	`fc21`	N/A
`.identity_work_city`	Identity.Attribute	Office City	N/A	`Madrid`	Updatable. Title cased
`.identity_work_country`	Identity.Attribute	Office Country	N/A	`Spain`	Updatable. Title cased
`.identity_nick`	Identity.Attribute	Nickname	N/A	`trent21`	Updatable
`.identity_bunit`	Identity.Attribute	General Information	N/A	N/A	Updatable
`.identity_category`	Identity.Attribute	User Category	N/A	N/A	Updatable
`.identity_cim_entity_zone`	Identity.Attribute	CIM Entity Zone	N/A	N/A	Updatable
`.identity_work_lat`	Identity.Attribute	Office Latitude	N/A	N/A	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.identity_work_long`	Identity.Attribute	Office Longitude	N/A	N/A	Updatable
`.identity_priority`	Identity.Attribute	User Criticality	N/A	N/A	Updatable
`.identity_first`	Identity.Attribute	First Name	N/A	N/A	Updatable
`.identity_last`	Identity.Attribute	Last Name	N/A	N/A	Updatable
`.identity_suffix`	Identity.Attribute	User Suffix	N/A	N/A	Updatable
`.identity_email`	Identity.Attribute	Email Address	N/A	N/A	Updatable
`.identity_phone`	Identity.Attribute	Phone Number	N/A	N/A	Updatable
`.identity_prefix`	Identity.Attribute	Role	N/A	N/A	Updatable
`.identity_start_date`	Identity.Attribute	User Start Date	N/A	N/A	Updatable
`.identity_end_date`	Identity.Attribute	User End Date	N/A	N/A	Updatable
`.identity_managed_by`	Identity.Attribute	Managed By	N/A	N/A	Updatable
`.asset_*`	Asset.Attribute	*	N/A	N/A	Updatable. All the keys that start with `asset_`
`.identity_*`	Identity.Attribute	*	N/A	N/A	Updatable All the keys that start with `Identity_`

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 minute
Assets	206
Asset Attributes	424
Identities	424
Identity Attributes	424

Change Log

- **Version 1.0.0**
    - Initial release