ThreatQuotient

SecurityScorecard CDF Guide

Version 1.0.0

April 11, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/securityscorecard-cdf

Introduction

The SecurityScorecard CDF for ThreatQ enables analysts to automatically ingest scorecard summaries and events into ThreatQ.

The integration provides the following feeds:

- **SecurityScorecard Summary Reports** - pulls scorecard reports for registered domains, into ThreatQ.
- **SecurityScorecard Events** - pulls events for a given domain.

The integration ingests the following system objects:

- Assets
  - Asset Attributes
- Events
  - Event Attributes
- Indicators
  - Indicator Attributes

Prerequisites

A Security Scorecard license & API key are required for this integration.

Asset Object

The integration requires the Asset object. The Asset installation files are included with the integration download on the ThreatQ Marketplace. The Asset object must be installed prior to installing the integration.

> ⚠ You do not have to install the Asset object if you are running ThreatQ version 5.10.0 or greater as the object has been seeded as a default system object.

Use the steps provided to install the asset custom object.

> ⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   <> cd /tmp/
   ```

4. Create a new directory:

   ```
   <> mkdir scorecard_cdf
   ```

5. Upload the **asset.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the scorecard_cdf directory.

   ```
   <> mkdir images
   ```

7. Upload the asset.svg
8. Navigate to the **/tmp/scorecard_cdf**.

   The directory should resemble the following:

- tmp
  - scorecard_cdf
    - asset.json
    - install.sh
    - images
      - asset.svg

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
<> chmod +x install.sh
```

10. Run the following command:

```
<> sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf scorecard_cdf
```

Installation

> The integration requires that the Asset object be installed on your ThreatQ instance prior to installing the CDF if your are on ThreatQ version 5.9.0 or earlier. Attempting to install or upgrade the CDF without the Asset object will cause the installation process to fail. See the Prerequisites chapter for more details.

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:

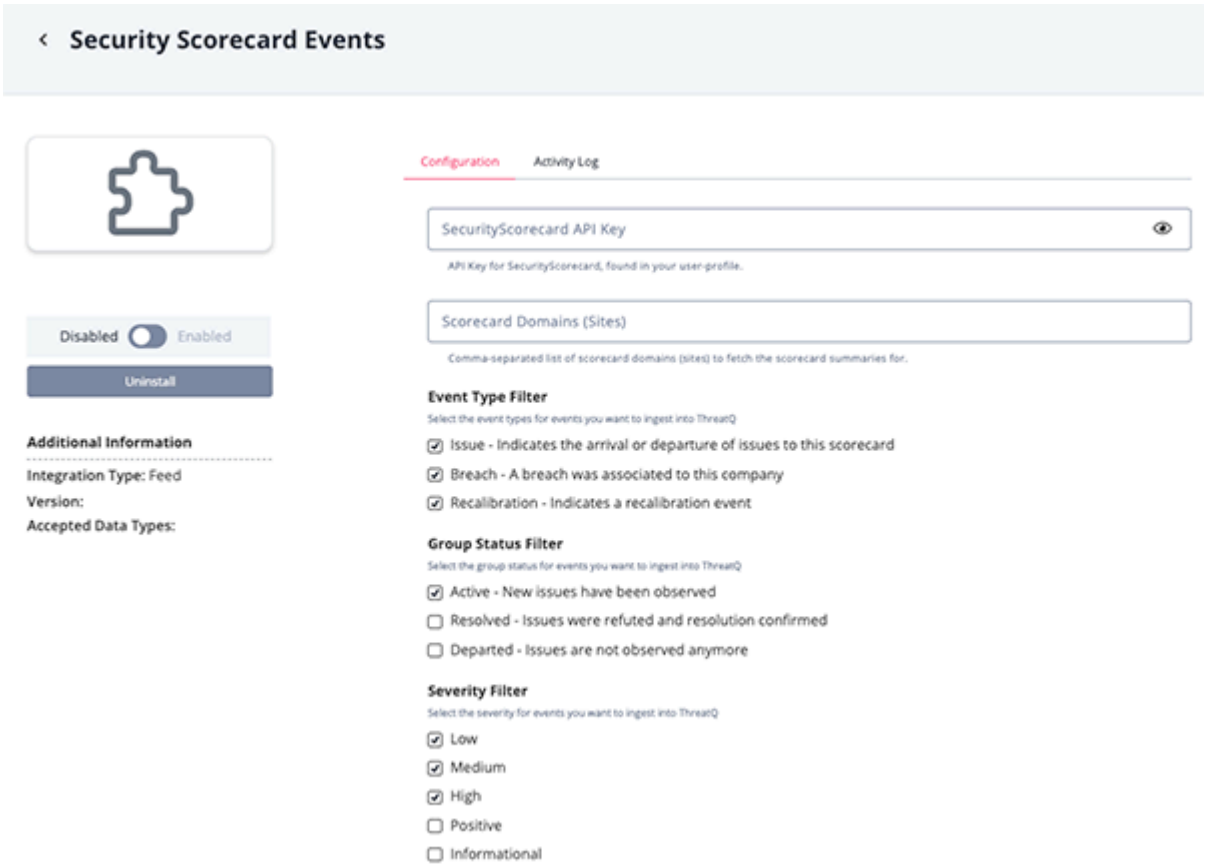
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

PARAMETER	DESCRIPTION
SecurityScorecard API Key	Your API Key for SecurityScorecard, found in your user-profile.
Scorecard Domains	A comma-separated list of scorecard domains (sites) to fetch the scorecard summaries.
Event Type Filter *(Scorecard Events feed only)*	Select the event types for events to ingest into ThreatQ. Options include: ◦ **Issue** - indicates the arrival or departure of issues to this scorecard (default) ◦ **Breach** - a breach was associated to this company (default) ◦ **Recalibration** - indicates a recalibration event (default)

PARAMETER	DESCRIPTION
Group Status Filter *(Scorecard Events feed only)*	Select the group status for events to ingest into ThreatQ. Options include ◦ **Active** - new issues have been observed (default) ◦ **Resolved** - issues were refuted and resolution confirmed (default) ◦ **Departed** - issues are not observed anymore (default)
Severity Filter *(Scorecard Events feed only)*	Select the severity for events to ingest into ThreatQ. Options include: ◦ Low (default) ◦ Medium (default) ◦ High (default) ◦ Positive ◦ Informational



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

Security Scorecard Summary Reports

The Summary Reports feed periodically pulls scorecard reports for registered domains into ThreatQ.

```
GET https://api.securityscorecard.io/companies/{{domain}}
```

Sample Response:

```
{
    "name": "ThreatQuotient Inc",
    "description": "",
    "domain": "threatq.com",
    "grade_url": "https://s3.amazonaws.com/ssc-static/grades/factor_a.svg",
    "industry": "information_services",
    "size": "unknown",
    "score": 91,
    "grade": "A",
    "last30day_score_change": -5,
    "is_entity": false,
    "is_un_published": true,
    "created_at": "2018-01-04T20:19:31.077Z",
    "disputed": false
}
```

ThreatQuotient provides the following default mapping for this feed:

> The `factors` key is data pulled from the **SecurityScorecard - Get Factors** supplemental feed

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.domain`	Asset Value	N/A	`.created_at`	`threatq.com`	N/A
`.factors[][.name,.grade,.score,.total_score_impact]`	Asset Description	N/A	N/A	SecurityScorecard Summary {{factors}}	The factors are built into an HTML description
`.domain`	Asset Attribute	Domain	N/A	`threatq.com`	N/A
`.description`	Asset Attribute	Description	N/A	N/A	This is different from the "built" description
`.disputed`	Asset Attribute	Is Disputed	N/A	False	Bool -> True/False
`.grade`	Asset Attribute	Grade	N/A	`A`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.score`	Asset Attribute	Score	N/A	`91`	N/A
`.industry`	Asset Attribute	Industry	N/A	`information_services`	N/A
`.last30day_score_change`	Asset Attribute	Last 30 Day Score Change	N/A	`-5`	N/A
`.name`	Asset Attribute	Scorecard Name	N/A	`ThreatQuotient Inc`	N/A
`.size`	Asset Attribute	Size	N/A	`unknown`	N/A

Security Scorecard Events

The Events feed periodically pulls events for a given domain. This includes breach events, recalibration events, new issue events, etc.

```
GET https://api.securityscorecard.io/companies/{{domain}}/history/events
```

Sample Response:


```
{
    "entries": [
        {
            "id": 1500171,
            "date": "2022-05-28T00:00:00.000Z",
            "event_type": "issues",
            "group_status": "departed",
            "issue_count": 1,
            "total_score_impact": 0,
            "issue_type": "service_vuln_host_info",
            "severity": "info",
            "factor": "patching_cadence",
            "detail_url": "https://api.securityscorecard.io/companies/threatq.com/history/events/2022-05-28/issues/
service_vuln_host_info?group_status=departed"
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

> The details key is data pulled from the **SecurityScorecard - Generic Request** supplemental feed, using this URL: `https://api.securityscorecard.io/companies/{{domain}}/factors`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.vulnerability_id`	Indicator Value	CVE	`.effective_date`	`CVE-2022-23943`	extracted from SecurityScorecard - Generic Request (Supplemental)
`.vulnerability_description`	Indicator Attribute	Description	`.effective_date`	`Product: Apache httpd\nSeverity: HIGH\nOut-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.`	extracted from SecurityScorecard - Generic Request (Supplemental)
`.vulnerability_url`	Indicator Attribute	External Reference	`.effective_date`	`https://nvd.nist.gov/vuln/detail/CVE-2022-23943`	extracted from SecurityScorecard - Generic Request (Supplemental)
`.details_url`	Asset Value	N/A	N/A	`threatq.com`	domain is extracted from detail_url after `/companies/`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.group_status,.factor,.issue_type,.severity`	Event Value	N/A	`.date`	`SecurityScorecard Departed Event: PATCHING CADENCE - service_vuln_host_info (Severity: Info)`	SecurityScorecard {{.group_status}} Event: {{.factor}} - {{.issue_type}} (Severity: {{.severity}})
`.details`	Event Description	Description	`.date`	SecurityScorecard - Generic Request (Supplemental) sample response `entries`	The evidence is put into `pre` tags for the description
`.event_type`	Event Type	N/A	`.date`	`Scorecard Issue`	map[`issues`] see below Event Table Mapping
`.detail_url`	Event Attribute	Domain	N/A	`threatq.com`	N/A
`.event_type`	Event Attribute	Event Type	N/A	`issues`	N/A
`.group_status`	Event Attribute	Group Status	N/A	`departed`	N/A
`.issue_count`	Event Attribute	Issue Count	N/A	`1`	N/A
`.total_score_impact`	Event Attribute	Total Score Impact	N/A	`0`	N/A
`.issue_type`	Event Attribute	Issue Type	N/A	`service_vuln_host_info`	N/A
`.severity`	Event Attribute	Severity	N/A	`info`	N/A
`.factor`	Event Attribute	Factor	N/A	`patching_cadence`	N/A

Event Table Mapping

ThreatQuotient provides the follow Event mapping:

KEY	VALUE
`issues`	`Scorecard Issue`
`breach`	`Breach`
`recalibration`	`Scorecard Recalibration`

SecurityScorecard - Get Factors (Supplemental)

This supplemental feed fetches "factors" for a given site's scorecard

`GET https://api.securityscorecard.io/companies/{{domain}}/factors`

Sample Response:


```
{
  "entries": [
        {
            "name": "application_security",
            "score": 71,
            "grade": "C",
            "grade_url": "https://s3.amazonaws.com/ssc-static/grades/factor_c.svg",
            "issue_summary": [
                {
                    "type": "csp_no_policy_v2",
                    "count": 1,
                    "severity": "medium",
                    "total_score_impact": 1.8012391326456623,
                    "detail_url": "https://api.securityscorecard.io/companies/threatq.com/issues/csp_no_policy_v2/"
                },
                {
                    "type": "csp_too_broad_v2",
                    "count": 4,
                    "severity": "low",
                    "total_score_impact": 2.2783649729965845,
                    "detail_url": "https://api.securityscorecard.io/companies/threatq.com/issues/csp_too_broad_v2/"
                }
      ]
    }
  ]
}
```


The mapping for this supplemental will be handled by the primary feed.

SecurityScorecard - Generic Request (Supplemental)

The Generic Requests supplemental feed fetches *any* data from the SecurityScorecard API.

`GET {{url}}`

Sample Response:

Using url=`https://api.securityscorecard.io/companies/threatq.com/history/events/2022-05-28/issues/service_vuln_host_info?group_status=departed`:


```
{
    "entries": [
        {
            "parent_domain": "threatq.com",
            "count": 1,
            "first_seen_time": "2022-05-25T02:43:02.000Z",
            "last_seen_time": "2022-05-25T02:43:02.000Z",
            "vulnerability_id": "CVE-2022-23943",
            "vulnerability_url": "https://nvd.nist.gov/vuln/detail/CVE-2022-23943",
            "vulnerability_description": "Product: Apache httpd\nSeverity: HIGH\nOut-of-bounds Write vulnerability in
mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This
issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.",
            "vulnerability_publish_date": "2022-03-14T00:00:00.000Z",
            "connection_attributes": {
                "protocol": "tcp",
                "dst_ip": "52.86.146.20",
                "dst_port": 443,
                "dst_host": "ec2-52-86-146-20.compute-1.amazonaws.com"
            },
            "effective_date": "2022-05-28T00:00:00.000Z",
            "group_status": "departed",
            "issue_id": "9651bf4c-6206-59ad-8c0f-9cba63ecf6b0"
        }
    ]
}
```


> The response for this supplemental feed will vary based on the URL. The mapping for this supplemental will be handled by the secondary feed.

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.

Summary Reports

METRIC	RESULT
Run Time	1 minute
Assets	1
Asset Attributes	8

Events

METRIC	RESULT
Run Time	1 minute
Assets	1
Events	42
Event Attributes	314
Indicators	21
Indicator Attributes	42

Change Log

- **Version 1.0.0**
  - Initial release