ThreatQuotient

Outseer CDF

Version 1.0.0

September 30, 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
ThreatQ Mapping 11
Outseer - Alerts 11
Average Feed Run 13
Known Issues / Limitations 14
Change Log 15

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	>= 5.26.0
Support Tier	ThreatQ Supported

Introduction

The Outseer CDF for ThreatQ enables users to retrieve alerts related to the user from the Outseer platform.

Outseer is leading the fight against payment fraud. Powered by cutting-edge data science and a suite of market-leading, anti-fraud products, Outseer reliably distinguishes authentic customers from fraudsters.

The integration provides the following feed:

- **Outseer - Alerts** - fetches Alerts related to the user from Outseer platform.

The integration ingests threat intel in the form of Event objects into the ThreatQ platform.

Prerequisites

The integration requires the following:

- Outseer Username
- Outseer Password
- Outseer Client 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
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.

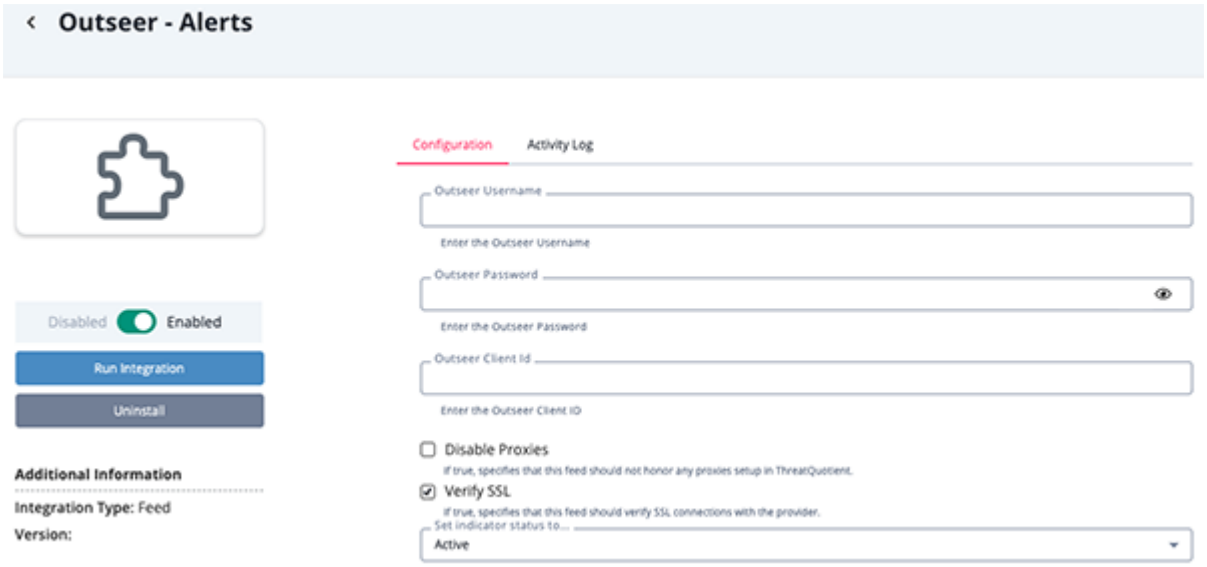
To configure the integration:

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
Outseer Username	Your Outseer Username.
Outseer Password	The password associated with the username supplied above.
Outseer Client ID	Your Outseer Client ID.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Verify SSL	When checked, validates the host-provided SSL certificate.



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

Outseer - Alerts

The Outseer - Alerts feed fetch Alerts from Outseer platform that are related to the user.

`POST https://api.dashboard.fraudaction.com/api/current-user/alerts/element/pending-shutdown-approvals`

Sample Response:


```
{
    "totalPagesCount": 1,
    "totalResultsCount": 3,
    "currentPage": 1,
    "items": [
        {
            "alertId": "213499",
            "severity": "HIGH",
            "alertTitle": "Action Required â€“ New Mobile Apps Detected",
            "alertType": "Pending Customer Approval",
            "read": false,
            "reportedTime": "09/12/2024 08:15:00 AM",
            "alertFields": {
                "trackingId": "4190-1000-00037",
                "resource": "https://sameapk.com/mygovid-
e3cb20e7bf563be5dae7dfc0b225f553/",
                "targetedBrandName": "Services Australia",
                "caseType": "Mobile Apps"
            }
        },
        {
            "alertId": "213482",
            "severity": "HIGH",
            "alertTitle": "Action Required â€“ New Mobile Apps Detected",
            "alertType": "Pending Customer Approval",
            "read": false,
            "reportedTime": "09/11/2024 02:45:00 PM",
            "alertFields": {
                "trackingId": "4190-1000-00036",
                "resource": "https://apk.plus/products_mygovid-
e3cb20e7bf563be5dae7dfc0b225f553-apk/",
                "targetedBrandName": "Services Australia",
                "caseType": "Mobile Apps"
            }
        },
        {
            "alertId": "213479",
```

```
            "severity": "HIGH",
            "alertTitle": "Action Required â€“ New Mobile Apps Detected",
            "alertType": "Pending Customer Approval",
            "read": false,
            "reportedTime": "09/11/2024 09:19:00 AM",
            "alertFields": {
                "trackingId": "4190-1000-00035",
                "resource": "https://apk.tools/details-mygovid-
e3cb20e7bf563be5dae7dfc0b225f553-apk/",
                "targetedBrandName": "Services Australia",
                "caseType": "Mobile Apps"
            }
        }
    ],
    "criteria": {
        "status": null,
        "showOnlyUnread": true,
        "reportTimeFrom": "09/11/2024",
        "reportTimeTo": "09/18/2024",
        "showOnlyPendingAction": false
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.items[].alertTitle + .items[].alertId`	Alert.Title	N/A	`.items[].reportedTime`	`Action Required - New Mobile Apps Detected - 213499`	We combine both keys to create an unique title
`.items[].alertFields.caseType`	Alert.Attribute	Case Type	`.items[].reportedTime`	`Mobile Apps`	N/A
`.items[].alertFields.resource`	Alert.Attribute	Resource	`.items[].reportedTime`	`https://sameapk.com/mygovid-e3cb20e7bf563be5dae7dfc0b225f553/`	N/A
`.items[].alertFields.targetedBrandName`	Alert.Attribute	Targeted Brand Name	`.items[].reportedTime`	`Services Australia`	N/A
`.items[].severity`	Alert.Attribute	Severity	`.items[].reportedTime`	`HIGH`	Updatable
`.items[].alertType`	Alert.Attribute	Alert Type	`.items[].reportedTime`	`Pending Customer Approval`	N/A

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	1 minute
Events	4
Event Attributes	20

Known Issues / Limitations

- The alerts retrieved from Outseer - Alerts are exclusive to the user set on the configuration page. Different users will have different alerts.
- Manual Runs - the maximum time frame you can pull with a manual run is 24 months due to a limitation with the Outseer API. Attempting a run with an time interval larger than 24 months will result in an error.

Change Log

- **Version 1.0.0**
  - Initial release