ThreatQuotient

CTM360 CyberBlindSpot CDF Guide

Version 1.0.0

March 14, 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	>= 4.58.1
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/ctm360-cyberblindspot-cdf

Introduction

The CTM360 CyberBlindSpot CDF ingests incidents and related indicators of compromise from CTM360 CyberBlindSpot.

The integration provides the following feed:

- **CTM360 CyberBlindSpot** - ingests incidents with related indicators of compromise.

The integration ingests the following system objects:

- Events - type Incident
- Indicators - FQDNs and URLs

Prerequisites

The integration requires an API key for CTM360 CyberBlindSpot.

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:

PARAMETER	DESCRIPTION
API Host	Your CTM360 hostname without https://.
API Key	Your CTM360 API Key.
Verify Host SSL	Enable or disable server certificate validation.

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

CTM360 CyberBlindSpot

The CTM360 CyberBlindSpot feed returns incidents and related IOCs (FQDN and URL).

`GET https://cbs.ctm360.com/api/v2/incidents`

Sample Response:

```
{
  "statusCode": 200,
  "success": true,
  "message": "Success",
  "incident_list": [
    {
      "id": "COMX414652011967",
      "subject": "https://pastebin.com/grgCciX8",
      "severity": "High",
      "type": "Exposed Email Address",
      "class": "URL",
      "status": "Member Feedback",
      "coa": "Takedown",
      "remarks": "New Exposed Email Address with severity High found",
      "created_date": "02-03-2023 04:35:36 PM",
      "updated_date": "02-03-2023 04:35:36 PM",
      "brand": "ISS Enterprise"
    },
    {
      "id": "COMX417109338865",
      "subject": "https://www.instagram.com/iss_elegant_enterprise",
      "severity": "Low",
      "type": "Brand Impersonation",
      "class": "URL",
      "status": "Under Analyst Review",
      "coa": "Monitoring",
      "remarks": "New Brand Impersonation with severity Low found",
      "created_date": "02-03-2023 02:06:22 PM",
      "updated_date": "02-03-2023 02:06:22 PM",
      "brand": "ISS Enterprise"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
incident_list[].subject	Indicators	FQDN or URL	https://pastebin.com/5uQpwnff	N/A	
{{data.remarks}} ({{data.subject}})	Event	event.title	New Exposed Email Address with severity High found (https://pastebin.com/5uQpwnff)	N/A	
incident_list[].id	Event Attributes	Incident ID	COMX412588498478	N/A	
incident_list[].severity	Event Attributes	Severity	High	N/A	
incident_list[].brand	Event Attributes	Brand	ISS Enterprise	N/A	
incident_list[].status	Event Attributes	Status	Member Feedback	N/A	
incident_list[].type	Event Attributes	Type	Exposed Email Address	N/A	
incident_list[].coa	Indicator Attributes	Course of Action	Takedown	N/A	

Change Log

- **Version 1.0.0**
  - Initial release