ThreatQuotient

Digital Shadows Incidents CDF User Guide

Version 1.1.0

October 18, 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	1.1.0
Compatible with ThreatQ Versions	>= 4.28.0
Support Tier	ThreatQ Supported

Introduction

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. It is an intelligence feed that provides detailed reports on, Incidents, Indicators and more.

As a Digital Shadows user, the integrations ingests Incidents and IOCs (that are found within an incident report) into the ThreatQ platform.

> Digital Shadows Incidents CDF replaced the Digital Shadows feed that was previously seeded in the ThreatQ platform (prior to ThreatQ v4.30).

Prerequisites

The DigitalShadows feed was renamed Digital Shadows Incidents and deployed as a configuration driven feed (CDF) with ThreatQ version 4.30.

After upgrading to ThreatQ version 4.30, the DigitalShadows feed will be renamed to Digital Shadows Incidents. Users that were using the DigitalShadows feed prior to upgrading will need to reenable the feed.

If you are installing the Digital Shadows Incidents feed on a platform version prior to 4.30 (using the yaml file from marketplace.threatq.com), the feed will install as a new feed and the existing DigitalShadows feed seeded with the platform will remain.

Digital Shadows Incidents objects will be ingested as ThreatQ incident objects by default. This setting can be updated to ingest objects as ThreatQ events, as the previous DigitalShadows feed operated, by updating the feed's configuration under the integration's details page.

The following attribute names will be migrated upon installing/updating the feed:

- Digital Shadows Severity -> Severity
- Digital Shadows Type -> Type
- Digital Shadows Score -> Score
- Digital Shadows URL -> URL
- Digital Shadows Received Time -> Verified At

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 ID	API ID provided by Digital Shadows. Necessary for authentication.
API Key	API key provided by Digital Shadows. Necessary for authentication.
Ingest as Incident Objects	If checked, ingests fetched incidents as ThreatQ Incident objects. Otherwise, fetched incidents are ingested as ThreatQ Event Objects. This parameter is checked by default.
Feed URL	For UI display purposes only.

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

Digital Shadows Incidents

Sample Response:


```
{
  "content": [
    {
      "id": 12345,
      "scope": "ORGANIZATION",
      "type": "DATA_LEAKAGE",
      "subType": "INTERNALLY_MARKED_DOCUMENT",
      "severity": "MEDIUM",
      "title": "Protectively marked document available on company site",
      "published": "2019-11-17T15:20:50.984Z",
      "summary": "Protectively marked document available on company site",
      "modified": "2019-11-17T15:20:50.984Z",
      "occurred": "2019-11-17T12:20:50.984Z",
      "verified": "2019-11-17T13:20:50.984Z",
      "tags": [
        {
          "id": 358,
          "name": "Protectively Marked Document",
          "type": "DATA_LEAKAGE"
        },
        {
          "id": 172,
          "name": "English",
          "type": "LANGUAGE"
        }
      ],
      "version": 1,
      "entitySummary": {
        "source": "www.slideshare.net/johnwynne/internal_review",
        "summaryText": "Strictly private and confidential.",
        "domain": "www.slideshare.net",
        "sourceDate": "2019-11-16T15:20:50.984Z",
        "screenshotId": "47d07513-db48-4589-b5d9-cad00ec1fe89",
        "screenshotThumbnailId": "1d5f6a48-3cec-4f3f-aa29-cef4d86ddaa4",
        "type": "WEB_PAGE",
        "fullText": "Strictly private and confidential. Not for distribution.
This material is provided to Addressee Only. ",
        "contentRemoved": false
      },
      "description": "Protectively marked document available on company site",
      "linkedContentIncidents": [
```

```
        {
          "id": 8363,
          "title": "Protectively marked document available on public site",
          "occurred": "2019-11-16T09:20:50.984Z",
          "severity": "HIGH",
          "scope": "ORGANIZATION"
        }
      ],
      "internal": true,
      "alerted": "2019-11-17T13:35:50.984Z",
      "mitigation": "If document is is not for publication, consider removing
from company site.",
      "impactDescription": "Protectively marked document exposed on public
website. Per the Severity Matrix, we assess the severity of this incident as
High since the protectively marked document is less than one year old, is
available for public consumption and review, and is explicitly marked
\"Strictly private and confidential\". ",
      "takedownRequestCount": 1,
      "review": {
        "note": "Incident actioned internally by Kim Bryon",
        "status": "CLOSED",
        "user": {
          "id": "3a49f01b-6863-468b-a963-b34c5fa87805",
          "fullName": "Sam Neil",
          "permissions": []
        },
        "created": "2019-11-17T15:20:50.747Z"
      }
    }
  ],
  "currentPage": {
    "offset": 3,
    "size": 20
  },
  "total": 200
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.content[].title	incident.value/ event.title	If ingesting event objects, the ThreatQ event type is `Incident`. N/A if ingesting incident objects.	.content[].published	Protectively marked document available on company site	(See `Notes` column)
.content[].published	incident.published_at/ event.published_at	N/A	N/A	2019-11-17T15:20:50.984Z	
.content[].occured	incident.attribute/ event.attribute event.happened_at	Occurred At	.content[].published	2019-11-17T15:20:50.984Z	
.content[].id	incident.attribute/ event.attribute	URL	.content[].published	12345	Attribute value generated from the following template: `https://portal-digitalshadows.com/client/incidents/{{id}}`
.content[].scope	incident.attribute/ event.attribute	Scope	.content[].published	ORGANIZATION	
.content[].type	incident.attribute/ event.attribute	Type	.content[].published	DATA_LEAKAGE	
.content[].subType	incident.attribute/ event.attribute	Subtype	.content[].published	INTERNALLY_MARKED_DOCUMENT	
.content[].severity	incident.attribute/ event.attribute	Severity	.content[].published	MEDIUM	
.content[].summary	incident.attribute/ event.attribute	Summary	.content[].published	Protectively marked document available on company site	
.content[].modified	incident.attribute/ event.attribute	Modified At	.content[].published	2019-11-17T15:20:50.984Z	
.content[].verified	incident.attribute/ event.attribute	Verified At	.content[].published	2019-11-17T15:20:50.984Z	
.content[].tags[]	incident.attribute/ event.attribute	Tag	.content[].published	`{id: 358, name: Protectively marked document, type: DATA_LEAKAGE}`	Each tag is a mapping, which is

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					used to construct a string in the form of `{{id}}, {{name}}, {{type}}`.
.content[].version	incident.attribute/ event.attribute	Version	.content[].published	1	
.content[].internal	incident.attribute/ event.attribute	Is Internal	.content[].published	true	
.content[].alerted	incident.attribute/ event.attribute	Alerted At	.content[].published	2019-11-16T09:20:50.984Z	
.content[].mitigation	incident.attribute/ event.attribute	Mitigation	.content[].published	"If document is not for publication, consider removing from public site."	
.content[].impact Description	incident.attribute/ event.attribute	Impact Description	.content[].published	"Per the Severity Matrix, we assess the severity of this incident as High since the protectively marked document is less than one year old, is available for public consumption and review, and is explicitly marked ""Strictly private and confidential""."	
.content[].takedown RequestCount	incident.attribute/ event.attribute	Takedown Request Count	.content[].published	1	
.content[].entity Summary.source	incident.attribute/ event.attribute	Entity Source	.content[].published	www.slideshare.net/johnwynne/ internal_review	
.content[].entity Summary.summary Text	incident.attribute/ event.attribute	Entity Summary	.content[].published	Strictly private and confidential.	
.content[].entity Summary.domain	incident.attribute/ event.attribute	Entity Domain	.content[].published	www.slideshare.net	
.content[].entity Summary.sourceDate	incident.attribute/ event.attribute	Entity Source Date	.content[].published	2019-11-16T15:20:50.984Z	
.content[].entity Summary.screenshot ThumbnailId	incident.attribute/ event.attribute	Entity Screenshot ID	.content[].published	1d5f6a48-3cec-4f3f-aa29-cef4d86ddaa4	
.content[].entity Summary.type	incident.attribute/ event.attribute	Entity Type	.content[].published	"WEB_PAGE"	
.content[].entityS ummary.fullText	incident.attribute/ event.attribute	Entity Text	.content[].published	Strictly private and confidential. Not for distribution.	
.content[].entity Summary.content Removed	incident.attribute/ event.attribute	Entity Content Removed	.content[].published	true	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.content[].review.note	incident.attribute/event.attribute	Review Note	.content[].published	Incident actioned internally by Bob Smith	
.content[].review.status	incident.attribute/event.attribute	Review Status	.content[].published	CLOSED	
.content[].review.user.id	incident.attribute/event.attribute	User ID	.content[].published	3a49f01b-6863-468b-a963-b34c5fa87805	
.content[].review.user.fullname	incident.attribute/event.attribute	User Name	.content[].published	Alice Kim	
.content[].review.user.permissions[]	incident.attribute/event.attribute	User Permissions	.content[].published	[]	
.content[].linkedContentIncidents[].title	incident.incident[].value/event.events[].title	If ingesting event objects, the ThreatQ event type is `Incident`. N/A if ingesting incident objects.	.content[].linkedContentIncidents[].occurred	Protectively marked document available on public site	
.content[].linkedContentIncidents[].id	incident.incident[].attribute/event.events[].attribute	URL	.content[].linkedContentIncidents[].occurred	8363	Attribute value generated from the following template: `https://portal-digitalshadows.com/client/incidents/{{id}}`
.content[].linkedContentIncidents[].occured	incident.incident[].attribute/event.events[].attribute incident.incident[].published_at/event.events[].published_at event.events[].happened_at	Occurred At	.content[].linkedContentIncidents[].occurred	2019-11-16T09:20:50.984Z	
.content[].linkedContentIncidents[].severity	incident.incident[].attribute/event.events[].attribute	Severity	.content[].linkedContentIncidents[].occurred	HIGH	
.content[].linkedContentIncidents[].scope	incident.incident[].attribute/event.events[].attribute	Scope	.content[].linkedContentIncidents[].occurred	ORGANIZATION	

Known Issues / Limitations

- The integration only supports a Start Date for manual runs and will use the current time as the End Date.

Change Log

- **Version 1.1.0**
  - Fixed an issue where a pagination error would sometimes keep a feed run from completing.
- **Version 1.0.1**
  - Fixed an issue where some attributes would display incorrectly.
- **Version 1.0.0**
  - Initial release