ThreatQuotient

Digital Shadows Incidents Feed Implementation Guide

Version 1.0.1

Monday, March 9, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Monday, March 9, 2020

Contents

Introduction

The Digital Shadows Incidents ingests Incidents into ThreatQ and relates IOCs that are found in an incident report into ThreatQ.

Data is ingested from the following endpoint:

- https://portal-digitalshadows.com/api/incidents/find

Versioning

- Current integration version: `1.0.1`
- Supported on ThreatQ versions `>= 4.28`

Data Migration

The DigitalShadows Incidents feed replaces the DigitalShadows feeds that was seeded with the TheatQ application prior to version 4.30.

The original DigitalShadows feed data was ingested into ThreatQ as event objects. The Digital Shadows Incidents feed ingests feed data as Incident objects by default.

> You can change the feed setting to ingest objects as ThreatQ events, as the previous DigitalShadows feed operated, by updating the feed’s configuration under Feed Settings.

The following attribute names will be migrated upon update:

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

Installation

The Digital Shadows Incidents feed is automatically installed when you upgrade your ThreatQ instance to version 4.30 or later. You can also install/upgrade the feed using the ThreatQ UI - see the steps below.

> Upon install, 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.

> The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Digital Shadows Incidents** feed file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

   The feed will be added to the **Commerical** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feeds under the **Commercial** tab.
3. Click on the **Feed Settings** link for each feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API ID	Provided by the vendor.
API Key	Provided by the vendor

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

The feed will ingest data from Digital Shadows' API

Sample

```
"content": [
    {
      "id": 12345,
      "scope": "ORGANIZATION",
      "type": "DATA_LEAKAGE",
      "subType": "INTERNALLY_MARKED_DOCUMENT",
      "severity": "MEDIUM",
      "title": "Protectively marked document available on company site",
      "published": "2019-10-29T09:03:08.795Z",
      "summary": "Protectively marked document available on company site",
      "modified": "2019-10-29T09:03:08.795Z",
      "occurred": "2019-10-29T06:03:08.795Z",
      "verified": "2019-10-29T07:03:08.795Z",
      "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": "2019-10-28T09:03:08.795Z",
        "screenshotId": "68599f0d-1a2f-4730-845e-
1a0d67316594",
        "screenshotThumbnailId": "00daa1be-a7fa-49d7-9ad0-
86bfca88cf2b",
        "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": "2019-10-28T03:03:08.795Z",
          "severity": "HIGH",
          "scope": "ORGANIZATION"
        }
      ],
      "internal": true,
      "alerted": "2019-10-29T07:18:08.795Z",
      "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": "a5d36d4a-6850-4314-8477-b2ac36a5b417",
          "fullName": "Sam Neil",
          "permissions": []
        },
        "created": "2019-10-29T09:03:08.548Z"
      }
    }
  ],
  "currentPage": {
    "offset": 3,
    "size": 20
  },
  "total": 200
}
```

ThreatQ Mapping

ThreatQ provides the following default mapping for this feed:

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Comment
Content		
URL	Event.Attribute or Incident.Attribute	https://portal-digitalshadows.com/client/incidents/{{id}}
Scope	Event.Attribute or Incident.Attribute	
Type	Event.Attribute or Incident.Attribute	
Subtype	Event.Attribute or Incident.Attribute	
Severity	Event.Attribute or Incident.Attribute	
Title	Event.value or Incident.value	Event Type == Incident
Summary	Event.Attribute or Incident.Attribute	
Modified At	Event.Attribute or Incident.Attribute	

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Comment
Occurred At	Event.Attribute and Event.happened_at or Incident.occurred_at	
Verified At	Event.Attribute or Incident.Attribute	
Tag	Event.Attribute or Incident.Attribute	
Version	Event.Attribute or Incident.Attribute	
Is Internal	Event.Attribute or Incident.Attribute	
Alerted At	Event.Attribute or Incident.Attribute	
Mitigation	Event.Attribute or Incident.Attribute	
Impact Description	Event.Attribute or Incident.Attribute	
Takedown Request Count	Event.Attribute or Incident.Attribute	
Entity Summary		
Entity Source	Event.Attribute or Incident.Attribute	

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Comment
Entity Summary	Event.Attribute or Incident.Attribute	
Entity Domain	Event.Attribute or Incident.Attribute	
Entity Source Date	Event.Attribute or Incident.Attribute	
Entity Screenshot ID	Event.Attribute or Incident.Attribute	
Entity Type	Event.Attribute or Incident.Attribute	
Entity Text	Event.Attribute or Incident.Attribute	
Entity Content Removed	Event.Attribute or Incident.Attribute	
Linked Content Incidents		

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Comment
URL	RelatedEvent.Attribute or RelatedIncident.Attribute	https://portal-digitalshadows.com/client/incidents/{{id}}
Related Event with the same Type, Unless given.	RelatedEvent.Title or RelatedIncident.Title	
Occurred At	RelatedEvent.Attribute or RelatedIncident.Attribute	
Severity	RelatedEvent.Attribute or RelatedIncident.Attribute	
Scope	RelatedEvent.Attribute or RelatedIncident.Attribute	
Review		
Review Note	Event.Attribute or Incident.Attribute	
Review	Event.Attribute or Incident.Attribute	

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Comment
Status		
User		
User ID	Event.Attribute or Incident.Attribute	
User Name	Event.Attribute or Incident.Attribute	
User Permissions	Event.Attribute or Incident.Attribute	

Change Log

- **Version 1.0.1**
  - Updated `.content[].tags[]` feed data path that if it does not contain all of the fields, (id, name, type), the value is omitted.
- **Version 1.0.0**
  - Initial Release