ThreatQuotient

IntelFinder CDF User Guide

Version 1.0.0

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	1.0.0
Compatible with ThreatQ Versions	>= 4.21.0
Support Tier	ThreatQ Supported

Introduction

IntelFinder is operated by Inteller ltd, an expert in web intelligence automation. They productized their proprietary technology, which has been used to serve Fortune 500 companies and government agencies for over 5 years, to create the world's first fully automated and scalable threat intelligence solution.

The IntelFinder CDF provides the following feed:

- **IntelFinder Alerts** - `https://dash.intelfinder.io/api.php`

The CDF ingests reports and report attributes into the ThreatQ platform.

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	The IntelFinder API Key for the account whose alerts will be fetched.

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

IntelFinder Alerts

`POST https://dash.intelfinder.io/api.php`

Sample Response:


```
{
  "code": 0,
  "alerts_number": 1,
  "alerts": [
    {
      "_id": "5d9dd07c1d41c80c1864b4a6",
      "subscription": "Domain Expiration",
      "priority": 3,
      "status": 1,
      "added_on": "2019-10-05 12:15:12",
      "last_update": "2019-10-05 12:15:12",
      "keyword": "google.com",
      "title": "A Domain is About to Expire",
      "description": "Please note that one of your domains is about to expire.",
      "details": "%elements%",
      "recommendation": "We recommend renewing the domain.",
      "base_elements": [
        {
          "label": "Domain",
          "value": "google.com"
        },
        {
          "label": "Expiration Date",
          "value": "September 30th, 2019"
        }
      ],
      "comments": [],
      "updates": [],
      "elements": [
        {
          "label": "Domain",
          "value": "google.com"
        },
        {
          "label": "Expiration Date",
          "value": "September 30th, 2019"
        }
      ]
    }
  ]
```

```
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.alerts[]._id	Report.Value, Report.Attribute	N/A	.alerts[].added_on	5d9dd07c1d41c70c1864b4a6	Report.Value Formatted as `{{.alerts[]._id}} - {{.alerts[].title}}`; Report.Attribute unformatted
.alerts[].title	Report.Value	N/A	.alerts[].added_on	A Domain is About to Expire	Formatted as `{{.alerts[].id}} - {{.alerts[].title}}`
.alerts[].description	Report.Description	N/A	N/A	Please note that one of your domains is about to expire.	
.alerts[].subscription	Report.Attribute	Subscription	N/A	Domain Expiration	
.alerts[].priority	Report.Attribute	Priority	N/A	Medium	Formatted as `[Very Low, Low, Medium, High, Urgent]` from `1-5`
.alerts[].indicator_status	Report.Attribute	Status	N/A	Active	Formatted as `[Active, Active, Expired, Expired, Whitelisted]` from `1-5`
.alerts[].keyword	Report.Attribute	Keyword	N/A	google.com	
.alerts[].images	Report.Attribute	Image	N/A		
.alerts[].link	Report.Attribute	Link			
.alerts[].elements[].value	Report.Attribute	.alerts[].elements[].label	September 30th, 2019	Attribute Key is dynamically set according to response data	

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.

IntelFinder Alerts

METRIC	RESULT
Run Time	< 1 minute
Reports	25
Report Attributes	400

Change Log

- **Version 1.0.0**
  - Initial release