ThreatQuotient

alphaMountain CDF

Version 1.0.0

May 29, 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

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.

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The alphaMountain CDF for ThreatQ enables the automatic ingestion of URLs with their corresponding categorizations and threat scores into the ThreatQ platform.

alphaMountain.ai provides up-to-date Domain and URL intelligence for cyber investigations and threat hunting. Using a combination of artificial intelligence and machine learning, alphaMountain.ai is able to provide fast and accurate contextualization for Domains and URLs.

The integration provides the following feeds:

- **alphaMountain Threat Categorizations** - pulls recently changed URLs with updates to their categorizations.
- **alphaMountain Threat Scores** - pulls recently changed URLs with updates to their threat scores.

The integration ingests URL and FQDN type indicators into the ThreatQ platform.

Prerequisites

The following is required in order utilize the integration:

- An alphaMountain.ai license.
- An alphaMountain.ai instance.

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. If prompted, select the individual feeds to install 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 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:

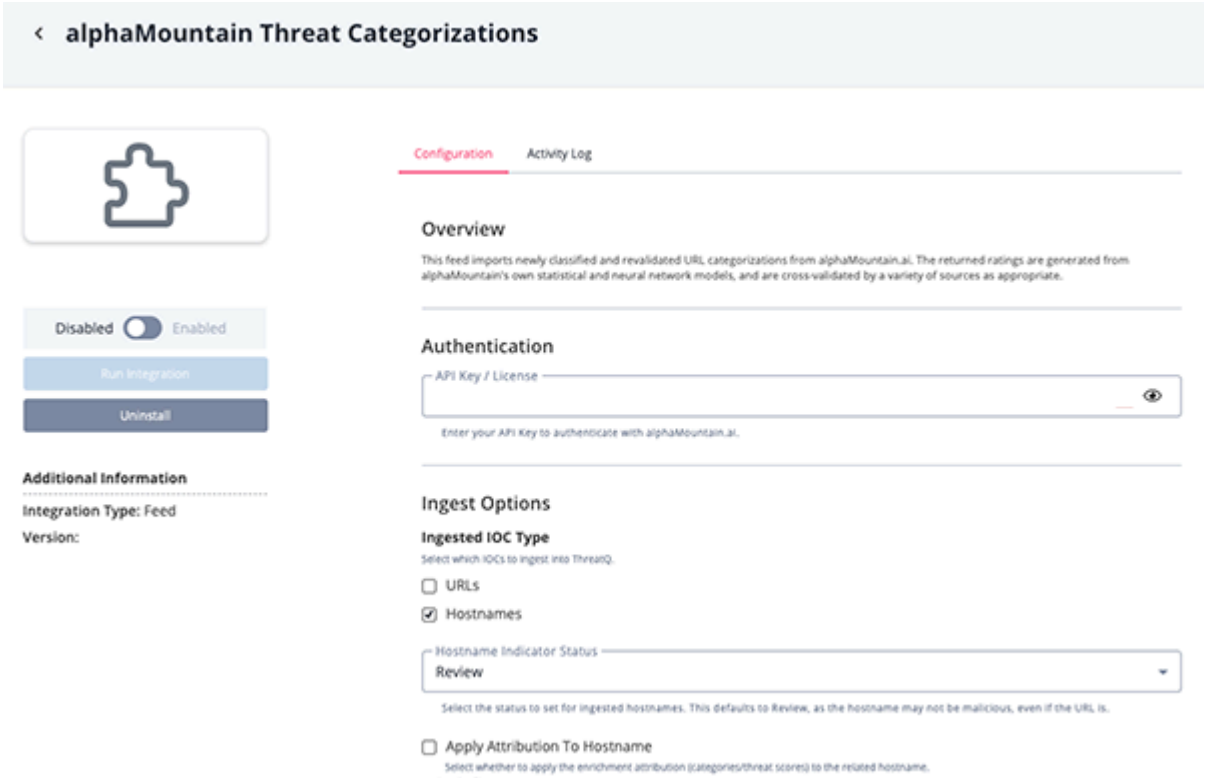
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

alphaMountain Threat Categorizations Parameters

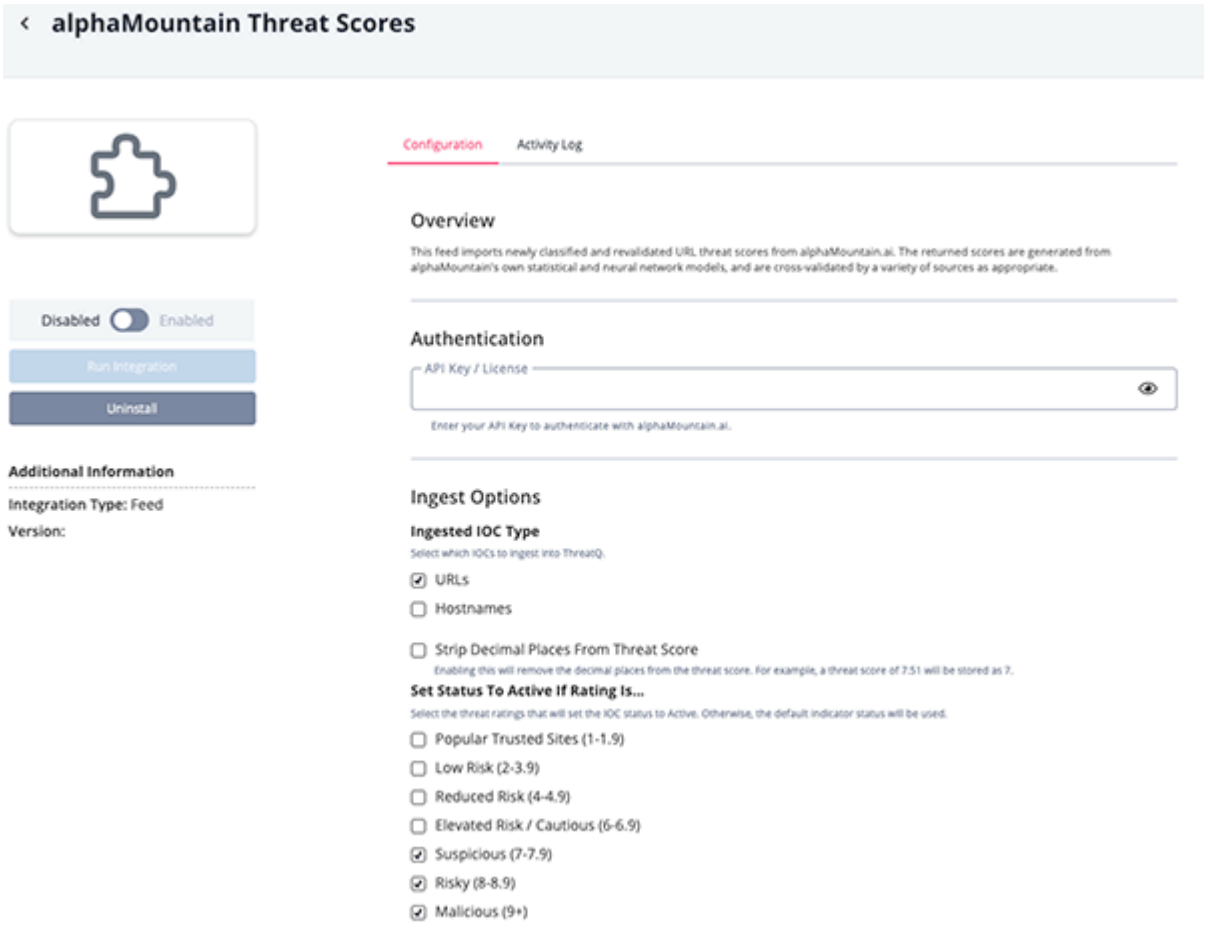
PARAMETER	DESCRIPTION
API Key	Enter your API Key to authenticate with alphaMountain.ai.
Ingested IOC Type	Select which IOCs to ingest into ThreatQ. Options include: ◦ URLs (default) ◦ Hostnames
Hostname Indicator Status	Select the status to set for ingested hostnames. This defaults to Review, as the hostname may not be malicious, even if the URL is. This field will only display if the `Hostnames` option is selected for the **Ingested IOC Type** field. Options include: ◦ Review (default) ◦ Active ◦ Indirect
Apply Attribution to Hostname	Enable/disable this option to apply the enrichment attribution (categories/threat scores) to the related hostname. This option is disabled by default.



alphaMountain Threat Scores Parameters

PARAMETER	DESCRIPTION
API Key	Enter your API Key to authenticate with alphaMountain.ai.
Ingested IOC Type	Select which IOCs to ingest into ThreatQ. Options include: ◦ URLs (default) ◦ Hostnames
Hostname Indicator Status	Select the status to set for ingested hostnames. This defaults to Review, as the hostname may not be malicious, even if the URL is. This field will only display if the `Hostnames` option is selected for the **Ingested IOC Type** field. Options include: ◦ Review (default) ◦ Active ◦ Indirect

PARAMETER	DESCRIPTION
Apply Attribution to Hostname	Enable/disable this option to apply the enrichment attribution (categories/threat scores) to the related hostname. This option is disabled by default.
Strip Decimal Places from Threat Score	Enabling this option will remove the decimal places from the threat score. This option is disable by default. **Example:** a threat score of 7.51 will be stored as 7.
Set Status to Active if Rating is...	Select the threat ratings that will set the IOC status to Active. Otherwise, the default indicator status will be used. Options include: ◦ Popular Trusted Sites (1-1.9) ◦ Low Risk (2-3.9) ◦ Reduced Risk (4-4.9) ◦ Elevated Risk / Cautious (6-6.9) ◦ Suspicious (7-7.9) (default) ◦ Risky (8-8.9) (default) ◦ Malicious (9+) (default)
Normalize Threat Score to Disposition	Enabling this option will add an additional attribute called **Disposition** to the ingested indicator records. The attribute will be a friendly representation of the Threat Score (ex: Malicious, Risky, Suspicious, Low Risk, Benign etc.). This option is enabled by default.



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

alphaMountain Threat Categorizations

The alphaMountain Threat Categorizations feed pulls URL indicators that have had recent changes to their categorizations. Category IDs will be normalized to their corresponding category names when ingested into ThreatQ.

```
POST https://batch.alphamountain.ai/category/feed/json
```

Sample Response:


```
{
  "version": 1,
  "status": {
    "category/feed": "Success"
  },
  "feed": [
    {
      "url": "http://01i.lol/",
      "hostname": "01i.lol",
      "categories": [51],
      "confidence": 0.90371
    },
    {
      "url": "http://02yuh9c.cn/",
      "hostname": "02yuh9c.cn",
      "categories": [39, 51],
      "confidence": 0.90371
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.url`	Indicator Value	`URL`	N/A	N/A	N/A
`.hostname`	Indicator Value	`FQDN`	N/A	N/A	Optional
`.categories[]`	Attribute	`Category`	N/A	`Malicious`	Normalized from the ID to the category name

alphaMountain Threat Scores

The alphaMountain Threat Scores feed pulls URL indicators that have had recent changes to their threat scores. Scores can be normalized to a verdict via the user configuration fields for more accurate mapping to your ThreatQ Scoring Policy.

`POST https://batch.alphamountain.ai/threat/feed/json`

Sample Response:


```
{
  "version": 1,
  "status": {
    "threat/feed": "Success"
  },
  "feed": [
    {
      "url": "http://qc8ki8mcb03udmn4vi9w.vus89.ru/",
      "hostname": "qc8ki8mcb03udmn4vi9w.vus89.ru",
      "score": 9.26
    },
    {
      "url": "http://teenpuppy.blogspot.com.cy/",
      "hostname": "teenpuppy.blogspot.com.cy",
      "score": 9.18
    },
    {
      "url": "http://whats-app-clone--oreolad2.repl.co/",
      "hostname": "whats-app-clone--oreolad2.repl.co",
      "score": 9.21
    },
    {
      "url": "http://info.eu/",
      "hostname": "info.eu",
      "score": 9.04
    },
    {
      "url": "http://marmenorboats.es/",
      "hostname": "marmenorboats.es",
      "score": 9.32
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on the items within the `.feed` array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.url`	Indicator Value	`URL`	N/A	N/A	N/A
`.hostname`	Indicator Value	`FQDN`	N/A	N/A	Optional
`.score`	Attribute	`Threat Score`	N/A	`9.18`	N/A
N/A	Attribute	`Disposition`	N/A	`Risky`	Optional; Enabled via a user-field

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.

alphaMountain Threat Categorizations

METRIC	RESULT
Run Time	1 minute
Indicators	105
Indicator Attributes	244

alphaMountain Threat Score

METRIC	RESULT
Run Time	41 minutes
Indicators	46,804
Indicator Attributes	140,631

Known Issues / Limitations

- The "limit" (maximum amount of URLs) per run is determined by your alphaMountain.ai license.

Change Log

- **Version 1.0.0**
  - Initial release