ThreatQuotient

DomainTools Brand Monitor CDF

Version 1.0.0

March 04, 2025

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	>= 6.3.0
Support Tier	ThreatQ Supported

Introduction

The DomainTools Brand Monitor CDF performs queries with the configured keywords against DomainTools Brand Monitor product and ingests the results. This allows security teams to search for potential typo squatting or brand-infringement domains.

The integration provides the following feed:

- **DomainTools Brand Monitor** - queries user supplied keywords against the Brand Monitor endpoint and ingests the results.

The integration ingests the following object types:

- Events
- Indicators
  - FQDN

Prerequisites

The following is required to run the integration:

- A DomainTools API username.
- A DomainTools API Key.

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

> 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:

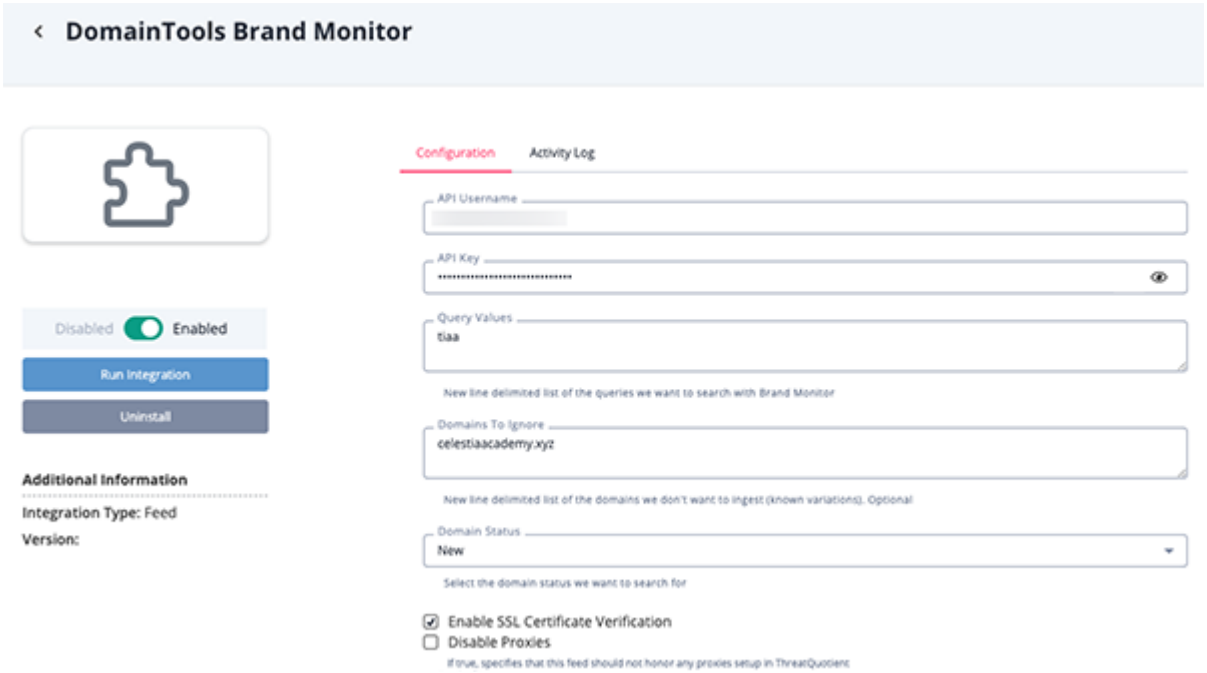
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

PARAMETER	DESCRIPTION
API Username	Your DomainTools API username.
API Key	Your DomainTools API Key.
Query Values	Enter a line-delimited list of keywords to query Brand Monitor. > The integration will perform an individual query for each keyword entered in this field.
Domains to Ignore	Optional - Enter a line-delimited list of domains that should not be ingested. These unwanted domains are referred to as variations.
Domain Status	Select the domain status to search for on Brand Monitor. Options include: ◦ Both *(default)* ◦ New ◦ On Hold
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.



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

DomainTools Brand Monitor

The DomainTools Brand Monitor feed queries user supplied keywords against the Brand Monitor endpoint and ingest the results.

> The integration will perform a query per keyword supplied. If multiple keywords are supplied, multiple queries will be performed.

```
GET https://api.domaintools.com/v1/mark-alert/
```

Sample Response:

```
{
    "query": "finance",
    "exclude": "auto|best",
    "new": true,
    "on-hold": true,
    "date": "2011-03-02",
    "total": 2,
    "alerts":
    [
        {
            "domain": "24hourfinance.info",
            "status": "on-hold"
        },
        {
            "domain": "actionis-finance.com",
            "status": "new"
        }
    ]
}
```

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[].domain`	Indicator Value	FQDN	`.date`	`24hourfinance.info`	N/A
`.query`	Indicator/Event Attribute	Brand Monitor Query	`.date`	`finance`	Updatable.
`alerts[].status`	Indicator/Event Attribute	Domain Status	`.date`	`on-hold`	Updatable. This is the registrar status, and must not be confused with Indicator Status
`.new`	Indicator/Event Attribute	Domain New	`.date`	`No`	Updatable. `Yes` if value is true, `No` if false
`.on-hold`	Indicator/Event Attribute	Domain On-Hold	`.date`	`Yes`	Updatable. `Yes` if value is true, `No` if false
`alerts[].domain`	Event Value	Alert	`.date`	`New match for "finance" for domain 24hourfinance.info`	N/A
`alerts[].domain`, `.query`	Event Description	N/A	`.date`	`24hourfinance.info detected by Brand Monitor against keyword "finance"`	Constructed as "`.alerts[].domain` detected by Brand Monitor against keyword `.query`"

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.

METRIC	RESULT
Run Time	1minute
Events	22
Event Attributes	88
Indicators	22
Indicator Attributes	88

Known Issues / Limitations

- Schedule your daily update to occur no sooner than 3am Pacific time for the best results. This ensures the data has been fully processed and is ready for your use. You will receive a 404 error response if the data has not been fully processed.
- Due to the nature that each query consumes resources, regardless of whether a match is found, your API account will be charged for each request you submit to the API. This is applicable even if are no domain names that match your query.

Change Log

- **Version 1.0.0**
  - Initial release