ThreatQuotient

A Securonix Company

Markdown to HTML Operation

Version 1.0.0

April 06, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.29.1
Support Tier	ThreatQ Supported

Introduction

The Markdown to HTML operation for ThreatQ enables users to seamlessly convert Markdown-formatted content into HTML compatible with ThreatQ's WYSIWYG editor. This functionality supports a wide range of Markdown elements, including headings, lists, links, images, tables, and code blocks, ensuring accurate formatting and presentation within the platform.

In addition to content conversion, users can define a source name and Traffic Light Protocol (TLP) designation for the generated description, allowing for proper attribution and classification of the ingested content.

The integration provides the following action:

- **Set Description** - converts Markdown-formatted text into HTML and applies it as a description to the specified ThreatQ object.

The integration is compatible with the following object types:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Courses Of Action
- Compromised Accounts
- Entities
- Events
- Exploits
- Targets
- Identities
- Incidents
- Infrastructure
- Intrusion Sets
- Malware
- Notes
- Reports
- Tools

- TTPs
- Vulnerabilities

Prerequisites

The following component is not required for installation of the operation but is optional:

- The Compromised Account custom object installed on your ThreatQ instance.

Compromised Account Custom Object

The integration is compatible with the Compromised Account custom object but does not require it, making this component optional for installation.

Use the steps provided to install the Compromised Account custom object.

> ⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Set your install pathway environment variable. This command will retrieve the install pathway from your configuration file and set it as variable for use during this installation process.

   ```
   INSTALL_CONF="/etc/threatq/platform/install.conf"

   if [ -f "$INSTALL_CONF" ]; then source "$INSTALL_CONF"

   fi

   MISC_DIR="${INSTALL_BASE_PATH:-/var/lib/threatq}/misc"
   ```

5. Navigate to the tmp folder using the environment variable:

```
cd $MISC_DIR
```

6. Upload the custom object files, including the images folder.

   The directory structure should resemble the following:

   - install.sh
   - <custom_object_name>.json
   - images (directory)
     - <custom_object_name>.svg

7. Run the following command:

   ```
   kubectl exec -it deployment/api-schedule-run -n threatq --
   sh /var/lib/threatq/misc/install.sh /var/lib/threatq/misc
   ```

   The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

8. Delete the install.sh, definition json file, and images directory from step 6 after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir markdown_op
   ```

5. Upload the **account.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the markdown_op directory.

```
mkdir images
```

7. Upload the account.svg.
8. Navigate to the **/tmp/markdown_op**.

   The directory should resemble the following:

   - tmp
     - **markdown_op**
       - **account.json**
       - **install.sh**
       - **images**
         - **account.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf markdown_op
```

Installation

> The operation requires the installation of the Compromised Account custom object before installing the actual operation. See the Compromised Account section of this guide for more details. The custom object must be installed prior to installing the operation. Attempting to install the operation without the custom object will cause the operation install process to fail.

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 zip file.
3. Extract the integration files and install the Compromised Account custom object if needed.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration whl 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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Set Description	Converts Markdown to HTML and sets it as the object's description	Account, Adversary, Asset, Attack Pattern, Campaign, Course Of Action, Entity, Event, Exploit Target, Identity, Incident, Infrastructure, Intrusion Set, Malware, Note, Report, Tool, TTP, Vulnerability	N/A

Set Description

The Set Description action converts Markdown-formatted text into HTML and applies it as a description to the specified ThreatQ object.

Run Configuration Options

These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this action:

PARAMETER	DESCRIPTION
Source Name	Optional - Specify a source name for the description entry. If not provided, the description's source will be set to `ThreatQ Platform`.
Source TLP	When setting the source for the description, you can also specify a TLP level. If not provided, the description will not have a TLP level associated with it.
Markdown Text	Enter the Markdown content to be converted to HTML and saved to the object.

Known Issues / Limitations

- If a description with the same source name already exists for the object, the **Set Description** action will overwrite it with the updated content.

Change Log

- **Version 1.0.0**
  - Initial release