ThreatQuotient

Cybereason Action User Guide

Version 1.0.0

February 26, 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

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.

Copyright © 2024 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	>= 5.26.0
Compatible with Cybereason Versions	>= 21.2.101
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Cybereason Action enables users to set a custom, organization-specific reputation (whitelist or blacklist) for IoCs.

The integration provides the following action:

- **Cybereason Set Reputation** - set reputation for IoCs in the Cybereason platform.

The action is compatible with the following Indicator types:

- MD5
- FQDN
- IP Address
- SHA-1

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - MD5
  - FQDN
  - IP Address
  - SHA-1
- A Cybereason username and password.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

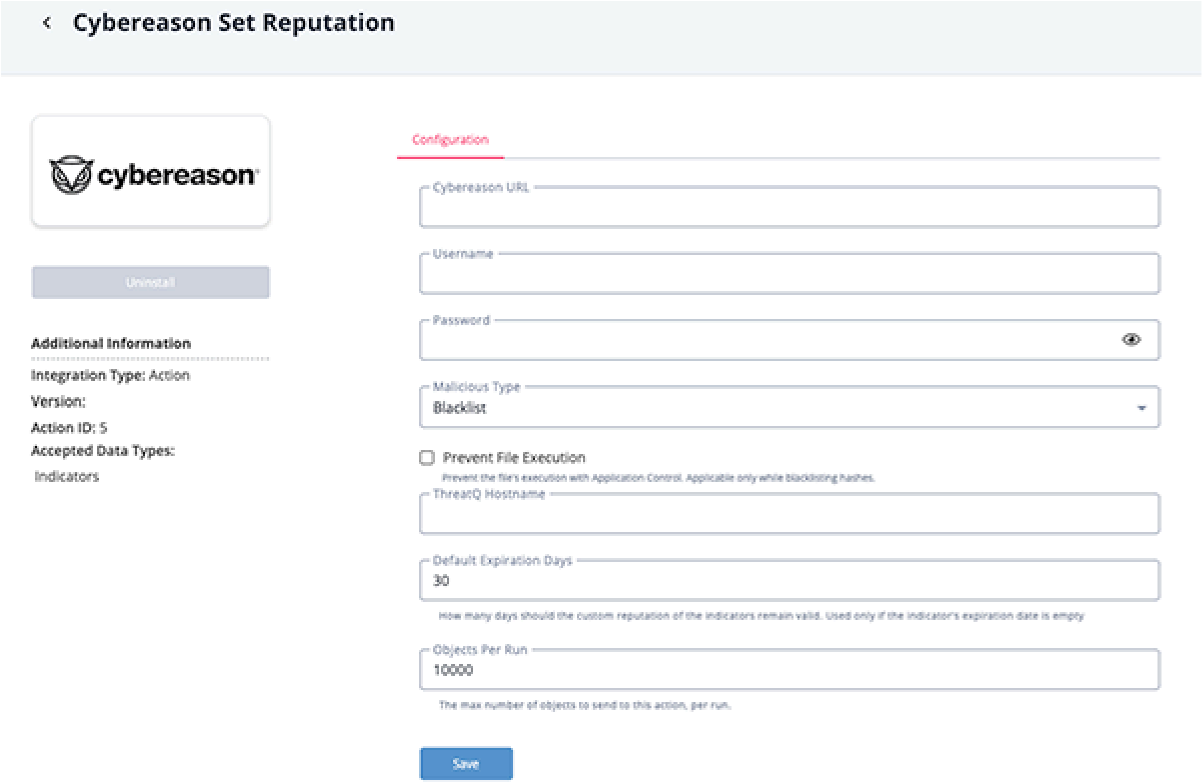
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Cybereason URL	Enter your Cybereason instance URL.
Username	Enter your Cybereason username.
Password	Enter your Cybereason password.
Malicious Type	Select the type to set for IOCs. Options include Whitelist and Blacklist.
Prevent File Execution	Enable this parameter to prevent the file's execution with Application Control. This is only applicable when blacklisting hashes.
ThreatQ Hostname	Enter your ThreatQ instance hostname or IP Address.

PARAMETER	DESCRIPTION
	This will be utilized when linking back to the ThreatQ instance.
Default Expiration Days	Enter how many days should the custom reputation of the indicators remain valid. This option is only used if the indicator's expiration date is empty
Objects per Run	Enter the max number of objects to submit per run.



‹ Cybereason Set Reputation

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Indicators

Configuration

Cybereason URL

Username

Password

Malicious Type: Blacklist

□ Prevent File Execution

Prevent the file's execution with Application Control. Applicable only while blacklisting hashes.

ThreatQ Hostname

Default Expiration Days: 30

How many days should the custom reputation of the indicators remain valid. Used only if the indicator's expiration date is empty

Objects Per Run: 10000

The max number of objects to send to this action, per run.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Cybereason Set Reputation	Sets the reputation for IoCs in the Cybereason platform.	Indicator	MD5, FQDN, IP Address, SHA-1

Cybereason Set Reputation

The Cybereason Set Reputation action sets the reputation, whitelist or blacklist, for IoCs on the Cybereason platform.

> This action does not ingest data back into the ThreatQ platform.

`POST {{CYBEREASON_URL}}/rest/classification/update`

Sample Request Parameters:

```
[
  {
    "comment": "Imported from ThreatQ: {{THREATQ_HOSTNAME}}/indicators/
{{INDICATOR_ID}} Score: 4 Sources: Threat Quotient",
    "expiration": 1709251200000,
    "keys": [
      "9a301f2a0259bdedb85e2ea4c071534776d471ab"
    ],
    "maliciousType": "blacklist",
    "prevent": true,
    "remove": false
  }
]
```

Sample Response:

```
{
  "outcome": "success",
  "data": true
}
```

Enriched Data

> Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	50

Use Case Example

1. A user identifies a group of MD5 and IP Addresses they want to set as Whitelisted on their Cybereason platform.
2. The user creates a data collection that contains those objects.
3. The user inserts that data collection into a workflow with the Cybereason action.
4. The user selects the Whitelist option for the Malicious Type configuration parameter.
5. The user saves and run the workflow.

Change Log

- **Version 1.0.0**
    - Initial release