ThreatQuotient

Cofense Triage Action Bundle User Guide

Version 1.0.0

October 10, 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	>= 5.20.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Cofense Triage Action Bundle provides actions that can be utilized to create or update Cofense Triage indicators.

The integration provides the following actions:

- **Cofense Triage - Create Indicators** - uploads indicators contained in a thread collection to Cofense Triage.
- **Cofense Triage - Update Indicators** - updates Cofense Triage indicators contained in a threat collection.

The action is compatible with the following indicator types:

- MD5
- URL
- FQDN
- SHA256

The action returns the following enriched indicator types:

- MD5
- URL
- FQDN
- SHA256

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 valid Cofense Client ID, Client Secret and base url for Cofense Triage.
- A data collection containing at least one of the following indicator types:
  - MD5
  - URL
  - FQDN
  - SHA256

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.

6. Select which actions to install and click on **Install**.

   You will still need to configure the action(s).

Configuration

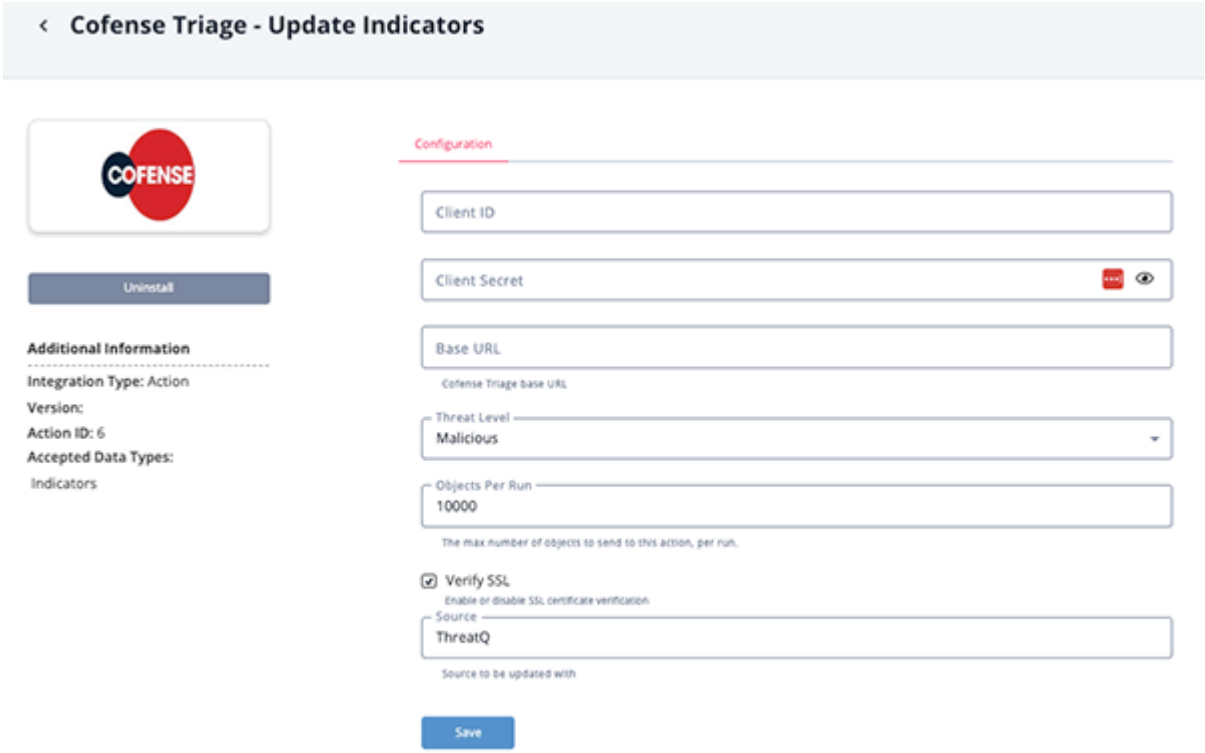
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
Client ID	Your Cofense Client ID.
Client Secret	Your Cofense Client Secret.
Base URL	Your Cofense Triage base URL.
Threat Level	Select the Threat Level to be set when creating a collection. Options include: ◦ Malicious (default) ◦ Suspicious ◦ Benign
Objects Per Run	Enter the max number of object to send per run. The default value is 10,000.
Verify SSL	Enable or disable SSL certificate verification.
Source *(Update Indicators action only)*	Enter the name of the source to be updated with.



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

Actions

The integration provides the following actions:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Cofense Triage - Create Indicators	Adds indicators to Cofense Triage.	Indicator	MD5, FQDN, URL, SHA256
Cofense Triage - Update Indicators	Updates indicators in Cofense Triage.	Indicator	MD5, FQDN, URL, SHA256

Cofense Triage - Create Indicators

The Cofense Triage - Create Indicators action creates indicators contained in a Cofense Triage thread collection.

`POST "{{base_url}}/api/public/v2/threat_indicators`

Sample Request:

```
{
  "data": {
    "type": "threat_indicators",
    "attributes": {
      "threat_level": "{{threat_level}}",
      "threat_type": "{{indicator_type}}",
      "threat_value": "{{indicator_value}}",
      "threat_source": "ThreatQ"
    }
  }
}
```

Sample Response:

```
    {
    "data": {
        "id": "325",
        "type": "threat_indicators",
        "links": {
            "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325"
        },
        "attributes": {
            "threat_level": "Benign",
            "threat_type": "SHA256",
            "threat_value":
"d9cd2a7965b72b5a02247dc580b6a75280ef8309ef58dcdc14152234d234d7f7",
            "threat_source": "ThreatQ",
            "created_at": "2021-06-11T06:39:47.376Z",
            "updated_at": "2022-05-25T10:59:21.546Z"
        },
        "relationships": {
            "owner": {
                "links": {
                    "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325/relationships/owner",
                    "related": "https://reltest6.phishmecloud.com/api/public/
v2/threat_indicators/325/owner"
                },
                "data": {
                    "type": "api_applications",
                    "id": "3"
```

```
                }
            },
            "reports": {
                "links": {
                    "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325/relationships/reports",
                    "related": "https://reltest6.phishmecloud.com/api/public/
v2/threat_indicators/325/reports"
                }
            },
            "comments": {
                "links": {
                    "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325/relationships/comments",
                    "related": "https://reltest6.phishmecloud.com/api/public/
v2/threat_indicators/325/comments"
                }
            }
        }
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value.id	Indicator.Attribute	ID	N/A	325	N/A
.value.attributes.threat_level	Indicator.Attribute	Threat Level	N/A	"Malicious"	N/A
.value.attributes.threat_source	Indicator.Attribute	Threat Source	N/A	"ThreatQ1"	N/A

Cofense Triage - Update Indicators

The Cofense Triage - Update Indicators action updates existing indicators contained in a Cofense Triage thread collection.

```
POST "{{base_url}}/api/public/v2/threat_indicators"
```

Sample Request:

```
{
  "data": {
    "type": "threat_indicators",
    "attributes": {
      "threat_level": "{{threat_level}}",
      "threat_type": "{{indicator_type}}",
      "threat_value": "{{indicator_value}}",
      "threat_source": "ThreatQ"
    }
  }
}
```

Sample Response:

```
{
    "data": {
        "id": "325",
        "type": "threat_indicators",
        "links": {
            "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325"
        },
        "attributes": {
            "threat_level": "Benign",
            "threat_type": "SHA256",
            "threat_value":
"d9cd2a7965b72b5a02247dc580b6a75280ef8309ef58dcdc14152234d234d7f7",
            "threat_source": "ThreatQ",
            "created_at": "2021-06-11T06:39:47.376Z",
            "updated_at": "2022-05-25T10:59:21.546Z"
        },
        "relationships": {
            "owner": {
                "links": {
                    "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325/relationships/owner",
                    "related": "https://reltest6.phishmecloud.com/api/public/
v2/threat_indicators/325/owner"
                },
                "data": {
                    "type": "api_applications",
                    "id": "3"
```

```
                }
            },
            "reports": {
                "links": {
                    "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325/relationships/reports",
                    "related": "https://reltest6.phishmecloud.com/api/public/
v2/threat_indicators/325/reports"
                }
            },
            "comments": {
                "links": {
                    "self": "https://reltest6.phishmecloud.com/api/public/v2/
threat_indicators/325/relationships/comments",
                    "related": "https://reltest6.phishmecloud.com/api/public/
v2/threat_indicators/325/comments"
                }
            }
        }
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value.attributes.threat_level	Indicator.Attribute	Threat Level	N/A	"Malicious"	Gets updated at each run
.value.attributes.threat_source	Indicator.Attribute	Threat Source	N/A	"ThreatQ1"	Gets updated at each run

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.

Confense Triage - Create Indicators

METRIC	RESULT
Run Time	1 minute
Indicators	6
Indicator Attributes	12

Confense Triage - Update Indicators

METRIC	RESULT
Run Time	1 minute
Indicators	10
Indicator Attributes	20

Known Issues / Limitations

- If the indicators from the collection are not validated by Cofense for any reason, Cofense responds with an `Unprocessable Entity` error. Example - if the **Cofense Triage - Create Indicators** action is run twice on the same collection, you will receive the error response for duplicated indicators. See the response log files for additional information.

Change Log

- **Version 1.0.0**
  - Initial release