ThreatQuotient

ThreatQ ACE Action User Guide

Version 1.1.2

November 01, 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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Actions **13**
ThreatQ ACE - Unstructured Intelligence Parser 13
Change Log **14**

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 © 2023 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	1.1.2
Compatible with ThreatQ Versions	>= 5.20.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ ACE Action is an action that utilizes the ThreatQ ACE Library to automatically parse context from data within ThreatQ.

The following action is provided:

- **ThreatQ ACE - Unstructured Intelligence Parser** - automatically parse context from data within ThreatQ.

The action is compatible with the following system object types:

- Malware
- Adversary
- Event
- Campaign
- Incident
- Attachment
- Report
- Tag

The action returns the following enriched system objects:

- Indicator
- Malware
- Adversary
- Attack Pattern
- Vulnerability
- Report
- Incident
- Campaign
- Event
- Attachment

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 object types:
  - Malware
  - Adversary
  - Event
  - Campaign
  - Incident
  - Attachment
  - Report
  - Tag

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 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:

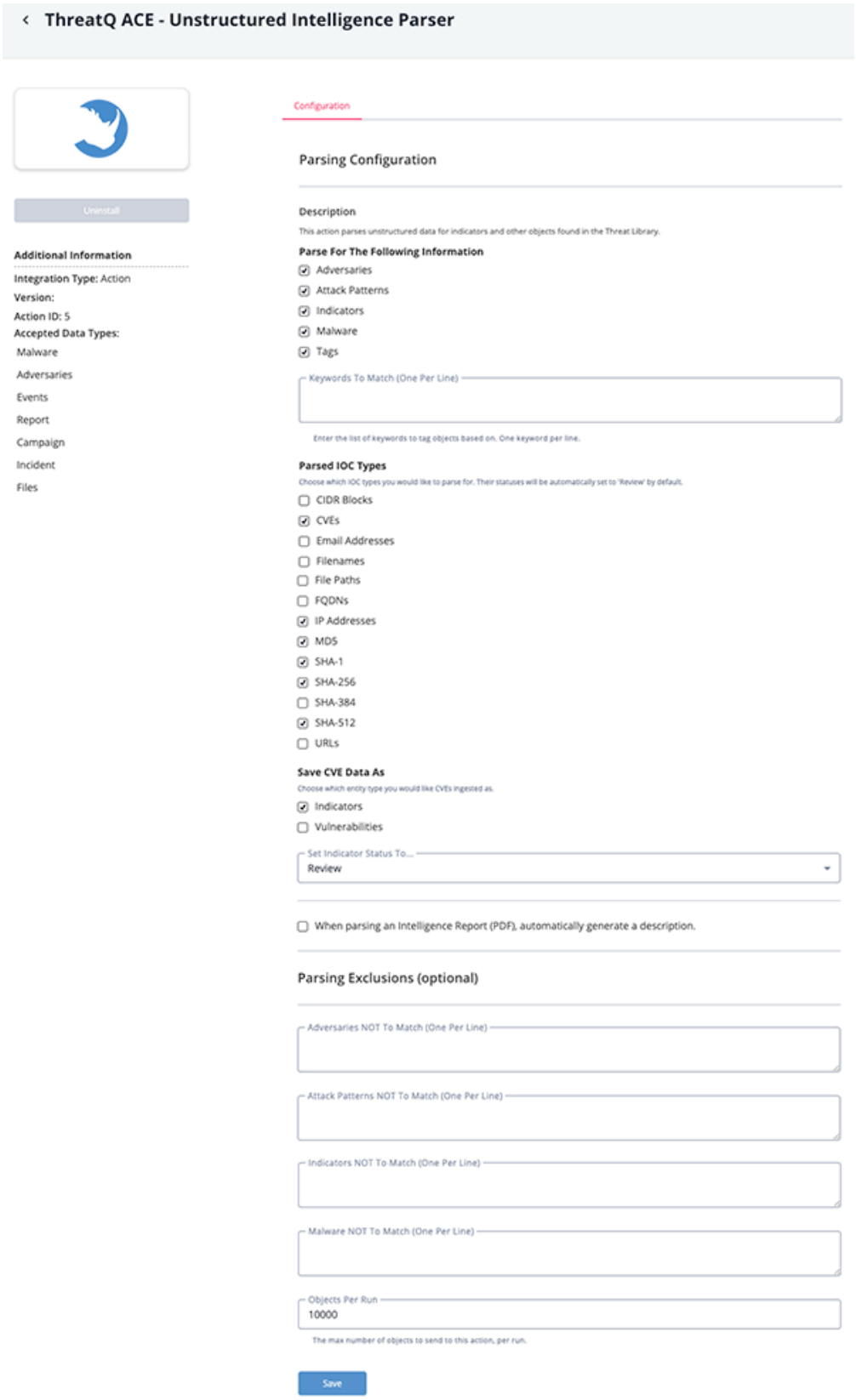
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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
Parse for the Following Information	Select the objects to parse. Options include: ◦ Indicators (default) ◦ Malware (default) ◦ Adversaries (default) ◦ Attack Patterns (default) ◦ Attributes (default) ◦ Tags (default)
Keywords to Match	Enter a list of keywords to tag objects based on. > This field will only be displayed if you have selected to parse for Tags.
Parsed IOC Types	Select the IOC types to parse. Options include: ◦ SHA-256 (default) ◦ SHA-512 (default) ◦ SHA-1 (default) ◦ SHA-384 ◦ MD5 (default) ◦ CIDR Blocks ◦ FQDNs ◦ URLs ◦ Filenames ◦ File Paths

PARAMETER	DESCRIPTION
	◦ CVEs (default) ◦ IP Addresses ◦ Email Addresses This field will only be displayed if you have selected to parse for Indicators.
Save CVE Data as	Select which entity type you would like CVEs ingested as. Options include **Indicators** (default) and **Vulnerabilities**. This field will only be displayed if you have selected to parse for Indicators.
Set Indicator Status to...	Select the status to apply to indicators.
Generate Description from PDF files	Enabling this will include the PDF's text in the Report's description.
Adversaries NOT to match	Optional - Enter the Adversary values not to parse. This field will only be displayed if you have selected to parse for Adversaries.
Attack Patterns NOT to match	Optional - Enter the Attack Pattern values not to parse. This field will only be displayed if you have selected to parse for Attack Patterns.
Indicators NOT to match	Optional - Enter the Indicators values not to parse. This field will only be displayed if you have selected to parse for Indicators.

PARAMETER	DESCRIPTION
Malware NOT to match	Optional - Enter the Malware values not to parse.  This field will only be displayed if you have selected to parse for Malware.
Vulnerabilities NOT to match	Optional - Enter the Vulnerability values not to parse.  This option will only appear if you have selected Vulnerabilities for the **Save CVE Data** as parameter.
Objects Per Run	The max number of objects to send to this action per run. The default value is **10,000**.



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

Actions

The following action is provided:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
ThreatQ ACE - Unstructured Intelligence Parser	Automatically parse context from data within ThreatQ	Malware, Adversary, Event, Campaign, Incident, Attachment, Report, Tag	N/A

ThreatQ ACE - Unstructured Intelligence Parser

The ThreatQ ACE - **Unstructured Intelligence Parser** action automatically parses context from selected data within ThreatQ.

> There is no mapping for this workflow. The ingested data depends on the selected objects & parsers.

Change Log

- **Version 1.1.2**
  - Resolved an issue where the action would not parse multiple tags.
- **Version 1.1.1**
  - The ACE Library and Filter are now seeded with the ThreatQ platform and no longer require manual installation. The integration has been updated to use those seeded files.
  - Updated minimum ThreatQ version to 5.20.0.
- **Version 1.1.0 rev-a**
  - Guide Update - updated ACE Library and Filter installation steps.
- **Version1.1.0**
  - Updated the action name from **Data Collection** to **Unstructured Intelligence Parser.**
  - Added the option to set indicator status.
  - Updated configuration parameters:
    - Added new parameter: **Set Indicator Status to...**
    - Renamed the **Selected Parsers** parameter to **Parse for the Following Information**.
    - Renamed the **Save PDF Text as Description** parameter to **Generate Description from PDF files**.
    - Renamed the **List of Keywords** parameter to **Keywords to Match**
    - Removed parameter: **Parsed Attributes**
    - Removed parameter: **Attribute Name**
    - Removed parameter: **Tag Entity Type**
- **Version 1.0.0**
  - Initial release