

ThreatQuotient



ThreatQ ACE Action User Guide

Version 1.1.0 rev-a

September 07, 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
 - ThreatQ ACE Library and ThreatQ ACE Filter 7
- Installation..... 9
- Configuration 10
- Action Functions 14
 - ThreatQ ACE - Unstructured Intelligence Parser 14
- Change Log 15

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	1.1.0
Compatible with ThreatQ Versions	>= 5.15
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
- ThreatQ ACE library and ThreatQ ACE Filter installed on your ThreatQ instance. These files are included in the marketplace download zip.

ThreatQ ACE Library and ThreatQ ACE Filter

The required ThreatQ ACE library and ThreatQ ACE Filter files are included in the action's marketplace download. Use the following steps to install the library.



When installing the library and filter, be aware that any in-progress feed runs will be cancelled when initiating step 8.

1. Locate the **tq_ace_filter-<version>-py3-none-any.whl** and **threatq_ace-<version>-py3-none-any.whl** files bundled with the marketplace zip file.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

```
cd /tmp/
```

4. Create a new directory:

```
mkdir ace_files
```

5. Navigate to this new directory:

```
cd ace_files
```

6. Upload the library and filter files to this directory.

7. Install the library and filter:

```
sudo -u apache /opt/threatq/python/bin/pip install threatq_ace-  
<version>-py3-none-any.whl  
  
sudo -u apache /opt/threatq/python/bin/pip install tq_ace_filter-  
<version>-py3-none-any.whl
```



If you encounter a permission error when running the commands above, run the following command:

```
chown apache:apache /tmp/ace_files/
```

After running the command, attempt the install commands again.

8. Restart Dynamo:

```
systemctl restart threatq-dynamo
```

9. Proceed with installing the action.

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.



This action download contains separate ThreatQ ACE Library and ThreatQ ACE Filter files that must be [installed via the command line](#). The ThreatQ ACE library and ThreatQ ACE Filter are required by the action and must be installed prior to attempting to use the action in a workflow.

3. Unzip the downloaded zip and extract the ThreatQ Ace Library, ThreatQ ACE Filter, and a second action zip file.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the extracted zip file (from step 3) 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	<p>Select the objects to parse. Options include:</p> <ul style="list-style-type: none"> ◦ Indicators (default) ◦ Malware (default) ◦ Adversaries (default) ◦ Attack Patterns (default) ◦ Attributes (default) ◦ Tags (default)
Keywords to Match	<p>Enter a list of keywords to tag objects based on.</p> <div>  <p>This field will only be displayed if you have selected to parse for Tags.</p> </div>
Parsed IOC Types	<p>Select the IOC types to parse. Options include:</p> <ul style="list-style-type: none"> ◦ SHA-256 (default) ◦ SHA-512 (default) ◦ SHA-1 (default) ◦ SHA-384 ◦ MD5 (default) ◦ CIDR Blocks ◦ FQDNs ◦ URLs ◦ Filenames ◦ File Paths

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ CVEs (default) ◦ IP Addresses ◦ Email Addresses <div>  This field will only be displayed if you have selected to parse for Indicators. </div>
Save CVE Data as	Select which entity type you would like CVEs ingested as. Options include Indicators (default) and Vulnerabilities . <div>  This field will only be displayed if you have selected to parse for Indicators. </div>
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. <div>  This field will only be displayed if you have selected to parse for Adversaries. </div>
Attack Patterns NOT to match	Optional - Enter the Attack Pattern values not to parse. <div>  This field will only be displayed if you have selected to parse for Attack Patterns. </div>
Indicators NOT to match	Optional - Enter the Indicators values not to parse. <div>  This field will only be displayed if you have selected to parse for Indicators. </div>

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

< ThreatQ ACE - Unstructured Intelligence Parser



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

Malware

Adversaries

Events

Report

Campaign

Incident

Files

Configuration

Parsing Configuration

Description

This action parses unstructured data for indicators and other objects found in the Threat Library.

Parse For The Following Information

- ☒ Adversaries
- ☒ Attack Patterns
- ☒ Indicators
- ☒ Malware
- ☒ Tags

Keywords To Match (One Per Line)

Enter the list of keywords to tag objects based on. One keyword per line.

Parsed IOC Types

Choose which IOC types you would like to parse for. Their statuses will be automatically set to 'Review' by default.

- ☐ CIDR Blocks
- ☒ CVEs
- ☐ Email Addresses
- ☐ Filenames
- ☐ File Paths
- ☐ FQDNs
- ☒ IP Addresses
- ☒ MD5
- ☒ SHA-1
- ☒ SHA-256
- ☐ SHA-384
- ☒ SHA-512
- ☐ URLs

Save CVE Data As

Choose which entity type you would like CVEs ingested as.

- ☒ Indicators
- ☐ Vulnerabilities

Set Indicator Status To...
Review

- ☐ When parsing an Intelligence Report (PDF), automatically generate a description.

Parsing Exclusions (optional)

Adversaries NOT To Match (One Per Line)

Attack Patterns NOT To Match (One Per Line)

Indicators NOT To Match (One Per Line)

Malware NOT To Match (One Per Line)

Objects Per Run
10000

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

Save

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

Action Functions

The following action is provided:

FUNCTION	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 1.1.0 rev-a**
 - Guide Update - updated ACE Library and Filter installation steps.
- **Version 1.1.0**
 - 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