ThreatQuotient

Trend Micro Vision One Action Bundle User Guide

Version 1.0.0

November 29, 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	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Trend Micro Vision One Action bundle enables the automatic dissemination of indicators to the Trend Micro Vision One platform. This action can be used to send items to the blacklist (suspicious object list), as well as the whitelist (exception list).

Trend Micro Vision One is a single and unified cybersecurity platform that provides XDR across cloud and on-premises environments. It provides a single view of all security alerts, prioritized based on risk, and actionable insights to speed up investigations and response.

The bundle provides the following actions:

- **Trend Micro VisionOne Add to Blocklist** - exports IOCs to the suspicious object blocklist in Vision One.
- **Trend Micro VisionOne Add to Exception List** - exports IOCs from the given Threat Library data collection to the exception list in Trend Micro Vision One.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- URL
- Email Address
- SHA-1
- SHA-256

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 Trend Micro Vision One API Key with the SOAR role.
- A data collection containing the indicators.

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.

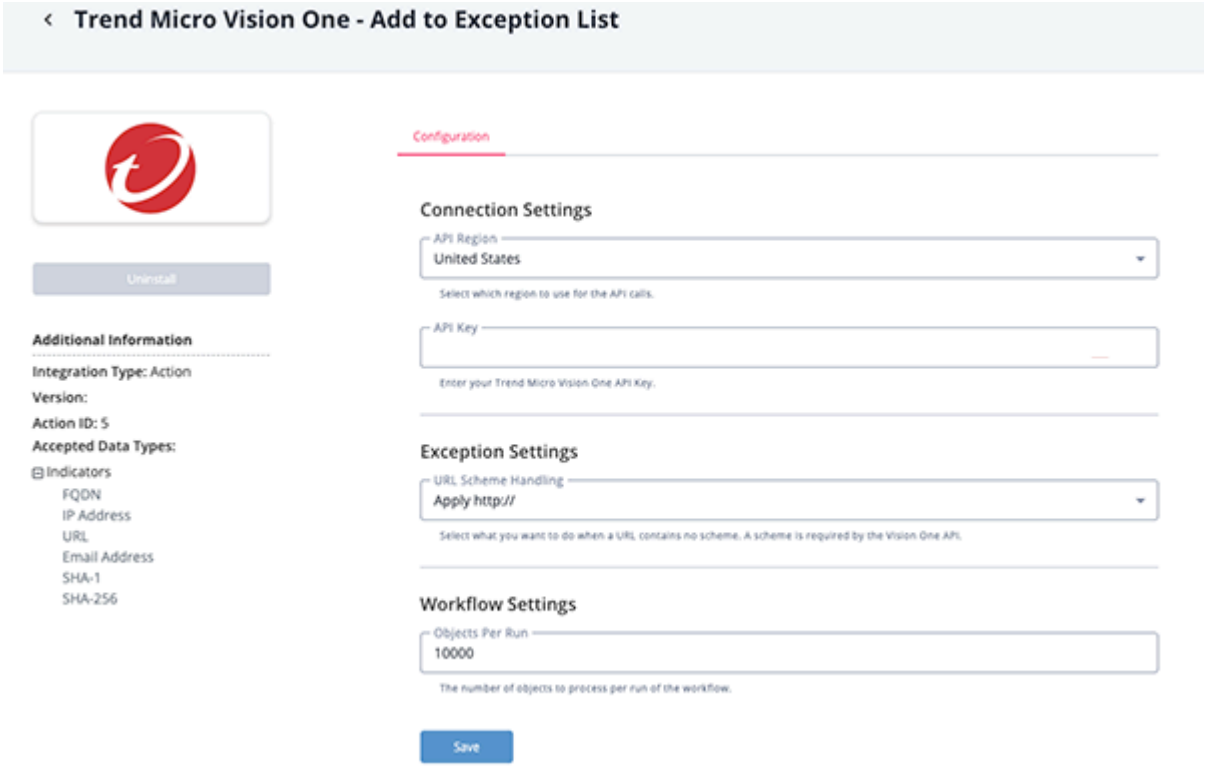
All Actions

PARAMETER	DESCRIPTION
API Region	Select which region to use for the API calls. Options include: ◦ United States ◦ European Union (EU) ◦ Australia ◦ Singapore ◦ Japan ◦ India
API Key	Enter your Trend Micro Vision One API Key. > This key must be from a SOAR role.
URL Scheme Handling	Select what you want to do when a URL contains no scheme. > A scheme is required by the Vision One API.

PARAMETER	DESCRIPTION
	Options include: ◦ Apply http:// (default) ◦ Apply https:// ◦ Add 2 IOCs (one with http:// and one with https:// ◦ Don't Send IOC
Objects Per Run	Enter the number of objects to process per workflow run.

Add to Blocklist - Additional Parameters

PARAMETER	DESCRIPTION
Scan Action	Select the action that connected products apply after detecting a suspicious object (IOC). Options include: ◦ Block (default) ◦ Log ◦ Based on Customer Settings
Risk Level	Select the risk level to apply to the suspicious objects (IOCs). Options include: ◦ Based on ThreatQ Score (default) ◦ High ◦ Medium ◦ Low ◦ Based on Customer Settings
IOC Expiration	Select the expiration date for the IOC . Options include: ◦ After 7 Days ◦ After 15 Days ◦ After 30 Days (default) ◦ After 45 Days ◦ After 60 Days ◦ After 75 Days ◦ After 90 Days ◦ Never ◦ Based on Customer Settings



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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Trend Micro Vision One - Add to Blocklist	Exports IOCs to the suspicious object blocklist in Vision One.	Indicator	FQDN, IP Address, URL, Email Address, SHA-1, SHA-256
Trend Micro Vision One - Add to Exception List	Exports IOCs to the exception list in Vision One.	Indicator	FQDN, IP Address, URL, Email Address, SHA-1, SHA-256

Add to Blocklist

The Add to Blocklist action exports IOCs from the given Threat Library data collection, to the suspicious object blocklist in Trend Micro Vision One. This action will give you the ability to choose how these IOCs are handled, including their risk level, their expiration, and more.

```
POST https://{{ api_region }}/v3.0/threatintel/suspiciousObjects
```

This action does not ingest data back into ThreatQ.

Add to Exception List

The Add to Exception List action exports IOCs from the given Threat Library data collection, to the exception list in Trend Micro Vision One.

```
POST https://{{ api_region }}/v3.0/threatintel/suspiciousObjectExceptions
```

This action does not ingest data back into ThreatQ.

Use Case Example

Trend Micro Vision One - Add to Blocklist

- Within ThreatQ, I have feeds and workflows setup to prioritize my IOCs. I want to be able to automatically export these IOCs to Trend Micro Vision One to be blocked.

Trend Micro Vision One - Add to Exception List

- Within ThreatQ, I curate a list of Whitelisted Domains, IP Addresses, and known good file hashes. I want to be able to automatically export these to Trend Micro Vision One's exception list.

Known Issues / Limitations

- Trend Micro Vision One has a limit of 10,000 suspicious objects (IOCs) per customer.
- This action will not export more than 10,000 IOCs to the blocklist.
- If you have more than 10,000 IOCs to export, you will need to refine your Threat Library data collection to limit the number of results.

Change Log

- **Version 1.0.0**
  - Initial release