ThreatQuotient

Joe Sandbox Operation Guide

Version 1.1.0

Tuesday, November 17, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 703.574.9893

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.

Contents

Versioning

- Integration Version: 1.1.0
- ThreatQ Version: 3.6 or greater

Introduction

The ThreatQuotient for Joe Sandbox Operation provides context in the form of attributes and indicators of compromise from the Cisco ThreatGrid API.

Preface

This guide provides the information necessary to implement the ThreatQuotient for Joe Sandbox Operation. This document is not specifically intended as a site reference guide.

It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

Audience

This document is intended for use by the following parties:

- ThreatQ and Security Engineers
- ThreatQuotient Professional Services Project Team & Engineers

Prerequisites

You must have a valid Cisco ThreatGrid API Key.

Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is strictly confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

Installation

Perform the following steps to install the integration:

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

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

You will still need to configure and then enable the operation.

Configuration

Note: *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 operation:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operations** option from the Category dropdown (optional).

   Note: *If you are installing the integration for the first time, it will be located under the Disabled tab.*
3. Click on the operation to open its details page.
4. Enter the following configuration parameter:

Parameter	Description
API Key	Your API Key from Joe Sandbox.

5. Click on the toggle switch, located above the Additional Information section, to enable it.
6. Click on **Save**.

Actions

The followings actions are available for the operation:

Action	Indicator Types	Description
Get URL Report	URL	Retrieves Reports from Joe Sandbox.
Submit URL Sample	URL	Submits a URL to Joe Sandbox for analysis.
Get File Report	File	Retrieves Reports from Joe Sandbox.
Submit File	File	Submits a File to Joe Sandbox for analysis.

Change Log

Version	Details
1.1.0	• Updated the integration to use the latest Joe Sandbox SDK v3.13.0. • Enhanced the exception handling, and added docstrings.
1.0.1	Initial Release