ThreatQuotient for Joe Sandbox Operation

December 7, 2018

Version 1.0.1

11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
https://www.threatq.com/
Support: support@threatq.com
Sales: sales@threatq.com

Contents

List of Figures and Tables

Introduction

1.1 Application Function

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

1.2 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.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

1.4 Scope

This document covers the implementation of the application only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Joe Sandbox Operation	1.0.1	

Implementation Overview

This document explains how to install and configure the ThreatQuotient for Joe Sandbox Operation found within the ThreatQ instance.

1.5 Prerequisites

 You must have a valid Cisco ThreatGrid API Key.

1.6 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.

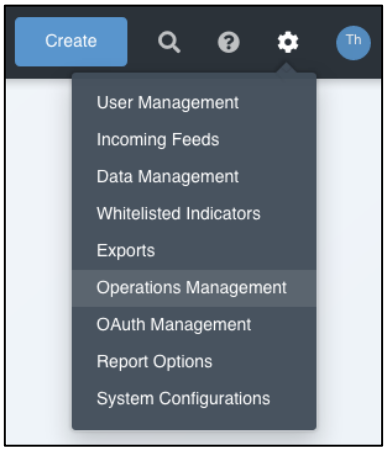
ThreatQuotient for Joe Sandbox Operation Installation

1.7 Setting up the Integration

Ensure the `tq_op_joe_sandbox-1.0.0-py3-none-any.whl` file is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for Joe Sandbox Operation is being installed/upgraded.

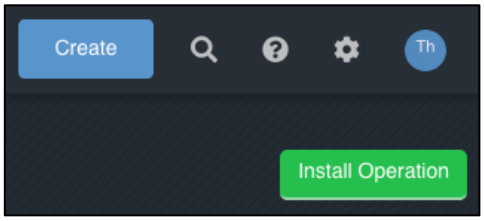
1. Navigate to the **Settings** icon > **Operations Management**.

Figure 1: Operations Management – Install



2. Click **Install Operation** in the upper right corner.

Figure 2: Install Operation



3. Drag the `tq_op_joe_sandbox-1.0.0-py3-none-any.whl` file to the **Add Operation** dialog box or select **click to browse** and navigate to the required file.

Figure 3: Add Operation

4. Click on the **Install** or **Upgrade** button.

Figure 4: Add Operation Process

Click on the install / upgrade.

You may be presented with **OPERATION ALREADY INSTALLED** as shown below.

Figure 5: Add Operation

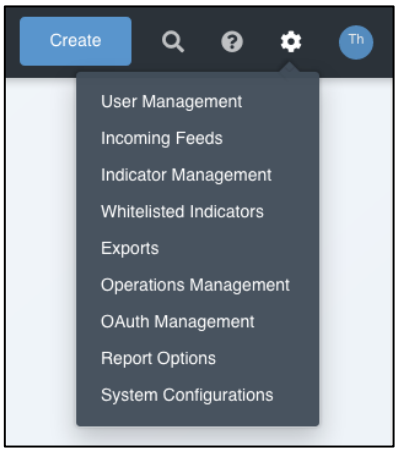
Installation / Upgrade is now complete.

1.8 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for Joe Sandbox Operation.

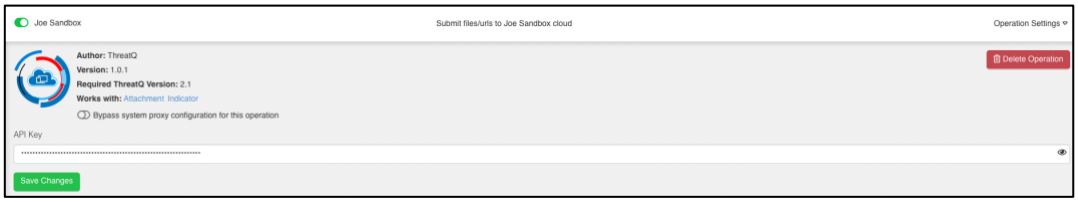
1. Navigate to the **Settings** icon > **Operations Management.**

Figure 6: Operations Management – Configuration



2. Expand the **Joe Sandbox** configuration.

Figure 7: Operation Configuration



3. Enter the API Key from Joe Sandbox into the **API Key** field.
4. Click **Save Change**.
5. Click the toggle button next to the **Joe Sandbox** name to enable the operation.

1.9 Actions

Table 2: Operation Actions Information

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

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.