ThreatQuotient

ThreatQuotient for FireEye EX Operation Guide

Version 1.0.0

Thursday, May 21, 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: 1.0.0
- ThreatQ Version: 4.31.0 or greater

Introduction

The ThreatQuotient for FireEye EX Operation allows a ThreatQ user to search for emails alerts in a FireEye EX appliance that contain specific indicators. If any alerts are returned, the data and indicators are parsed and listed in the ThreatQ UI.

Preface

This guide is to provide the information necessary to implement the ThreatQuotient for FireEye EX Operation. This document is not specifically intended to form 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:

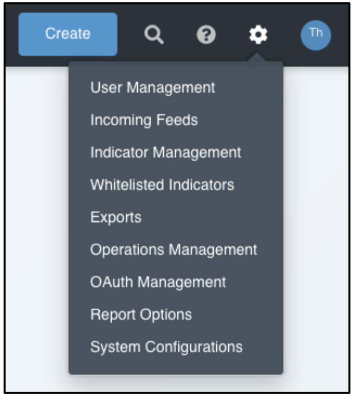
1. ThreatQ and Security engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

Installation

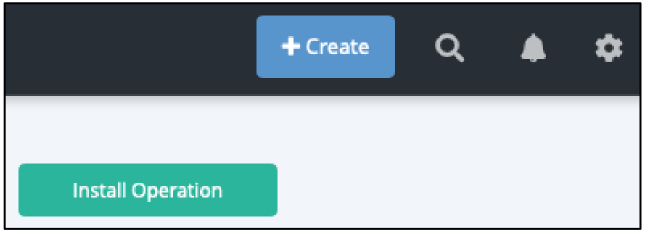
Perform the following steps to install the operation:

> ***Note:*** *The same steps can be used to upgrade the operation to a new version.*

1. Ensure the .whl file is available on the device being used to administer the ThreatQ instance in which the FireEye EX Operation is being installed/upgraded.
2. Log into your ThreatQ instance.
3. Click on the **Settings** icon and select **Operations Management**.



4. Click on the **Install Operation** button.



5. Upload the operation file using one of the following methods:

- Drag and drop the file into the dialog box.
- Select Click to Browse to locate the operation file on your local machine.

Note: ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding.

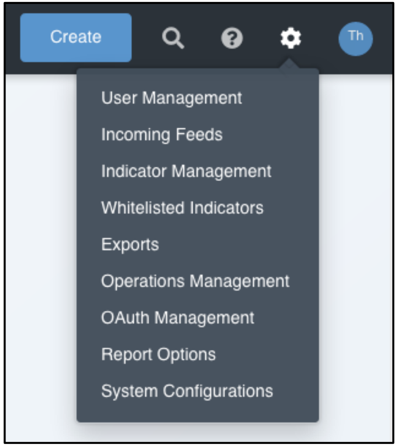
The operation will be added to your list of installed operations. You will still need to configure and enable the operation.

Configuration

__Note:__ ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other operation-related credentials.

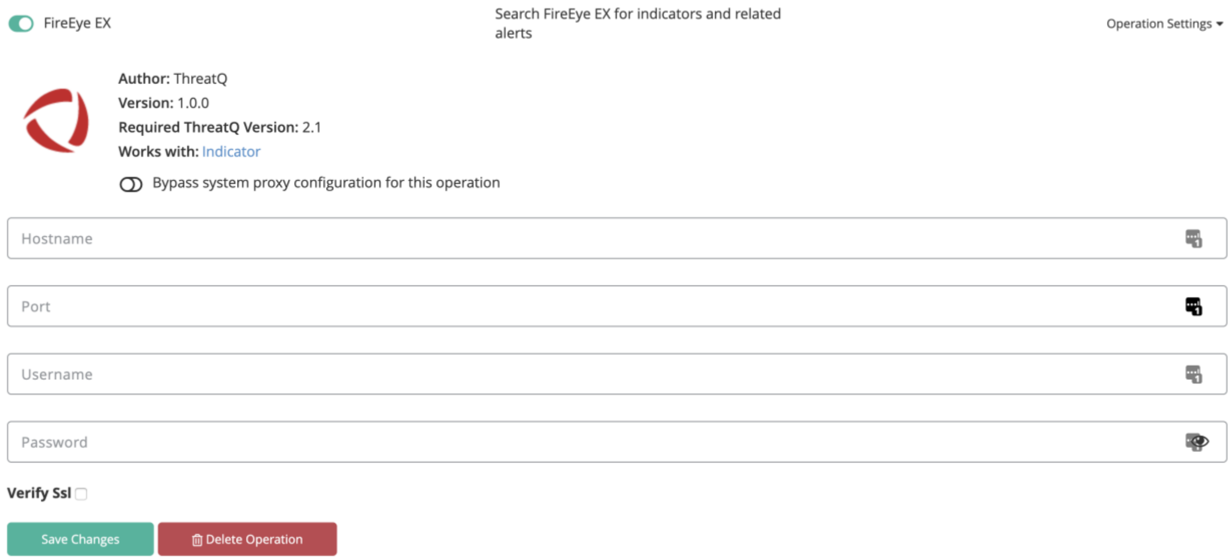
To configure the operation:

1. Click on the **Settings** icon and select **Operations Management**.



2. Locate the operation and click on **Operation Settings**.
3. Enter the following configuration parameters:

Parameter	Description
Hostname	Hostname or IP address of FireEye EX.
Port	Communication port (default is 443).
Username	Username for connecting to FireEye.
Password	Password for authenticating with FireEye
Verify SSL	Check this box to verify SSL when connecting to the FireEye EX instance.



FireEye EX

Search FireEye EX for indicators and related alerts

Operation Settings ▾

Author: ThreatQ
Version: 1.0.0
Required ThreatQ Version: 2.1
Works with: Indicator

Bypass system proxy configuration for this operation

Hostname

Port

Username

Password

Verify Ssl □

4. Click on **Save Changes**.
5. Click on the toggle switch to the left of the connector name to enable the connector.

Usage

The operation can be executed on the following ThreatQ objects: URL, MD5, Email Address, Filename and Malware name.
The operation supports different filters for each of the objects it is executed on. The following table lists the supported filters.

Object Type	Action	Supports Time Filtering	Supports Alert ID Filtering (optional)
URL	Search for alerts containing URL	Yes	Yes
MD5	Search for alerts that contain MD5 hash	No	Yes
Email Address	Search for alerts that match the email address of the malware object sender	No	Yes
Filename	Search for alerts that contain a malware filename that matches the ThreatQ indicator	Yes	Yes
Malware Name	Search for alerts that contain a specific malware	Yes	Yes

Change Log

Version	Details
1.0.0	Initial Release