ThreatQuotient

ThreatQuotient for AlienVault OTX Pulse Operation Guide

Version 1.0.1

Thursday, March 12, 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.

Last Updated: Thursday, March 12, 2020

Contents

Introduction

TheThreatQuotient forAlienVault OTXPulse Operationallows a ThreatQ user to query Ali-enVault for any indicator matches. If matches are found, related indicators will be returned, as well as any related pulses.

Preface

This guideprovidesthe information necessary to implementthe ThreatQuotient forAlienVault OTXPulse Operation.This document is not specifically intended asa site reference guide.It is assumed that the implementation engineer has experience installing and commissioningthe ThreatQuotient Apps and integrations covered within the document, as well as the exper-iencenecessary to troubleshoot at a basic level.

Audience

This document is intended for use by the following parties:

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

Scope

This document covers the implementation of the ThreatQuotient for AlienVault OTX Pulse Operation only.

Software/App Name	Version
ThreatQ	Version 4.20 or greater
ThreatQuotient for AlienVault OTX Pulse Operation	1.0.1

Installation

Perform the following steps to install the operation:

> 📝 The same steps can be used to upgrade the operation to a new version.

1. Log into https://marketplace.threatq.com/.

2. Locate and download the **AlienVault OTX Pulse Operation** file.

3. Navigate to your ThreatQ instance.

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

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

6. 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

   > 📝 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 then enable the operation.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.

To Configure the AlienVault OTX Pulse Operation:

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

2. Locate the **AlienVault OTX Pulse** operation and click on **Operation Settings**.

3. Enter the following parameter for the operation:

 | Parameter | Details |
   |-----------|---------|
   | Token | Your AlienVault OTX PulseAPI Key. |

4. Click on **Save Changes** then click on the toggle switch next to the operation name to enable the operation.

Usage

The following section covers the use of the ThreatQuotient for AlienVault OTX Pulse Operation.

Query

This action will query AlienVault OTX for any metadata, related indicators, and related pulses.
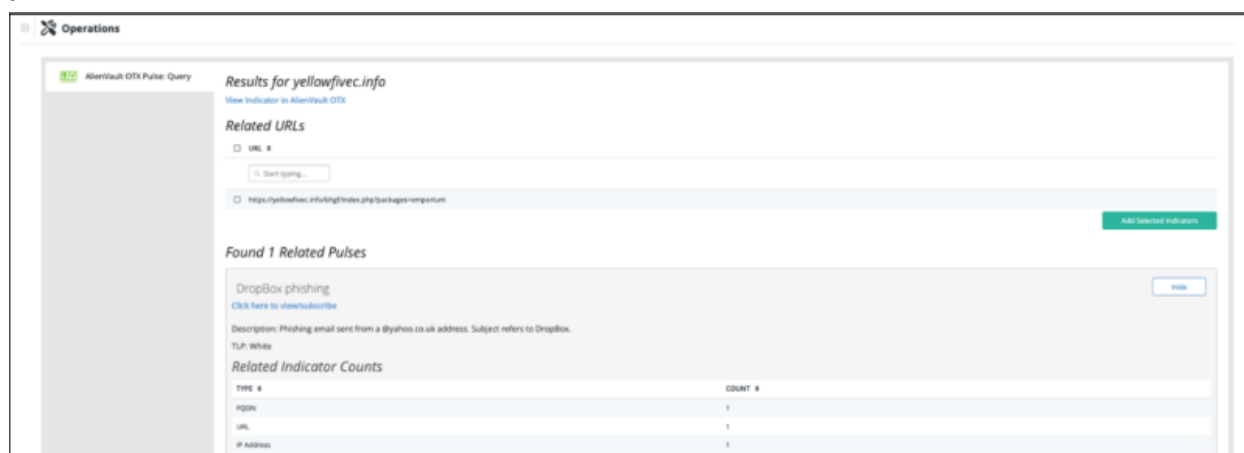
Change Log

- **Version 1.0.1**

    - Improved Proxy Support

- **Version 1.0.0**

    - Initial Release