ThreatQuotient

ThreatQuotient for Tenable.io Operation

Version 1.0.0

April 23, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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: Friday, April 23, 2019

Contents

List of Figures and Tables

Introduction

1.1 Application Function

The ThreatQuotient for Tenable.io Operation queries Tenable.io for vulnerable hosts in an organization's environment. Tenable.io scans hosts and networks for vulnerabilities; this operation pulls scan reports about vulnerable hosts into ThreatQ.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Tenable.io Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

- ThreatQ and Security Engineers
- 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

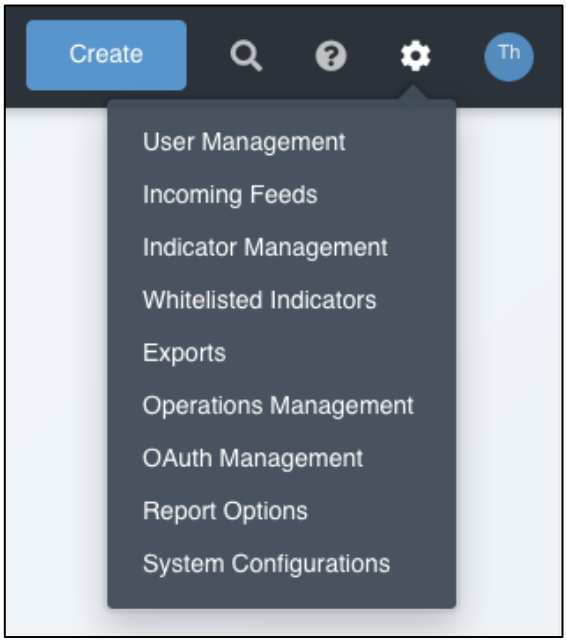
Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Tenable.io Operation	Version 1.0.0	

1.5 Setting up the Integration

Ensure the file `tq_op_tenable_io-1.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for Tenable.io Operation is being installed or upgraded.

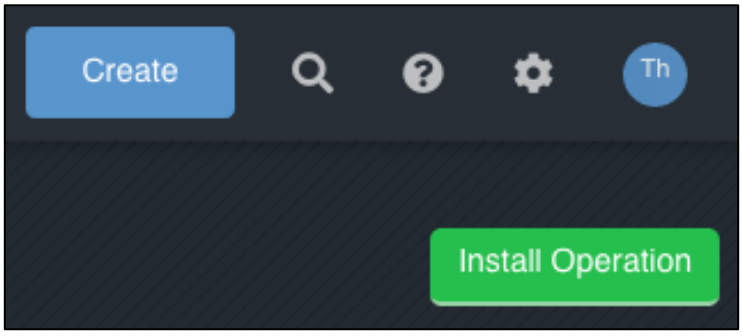
1. Navigate to the **Settings icon** > **Operations Management.**

Figure 1: Operations Management – Install



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

Figure 2: Install Operation



3. Drag the `tq_op_tenable_io-1.0.0-py3-none-any.whl` to the Add Operation Popup or **Click to Browse** to the required file.

Figure 3: Add Operation

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

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

Figure 4: Add Operation

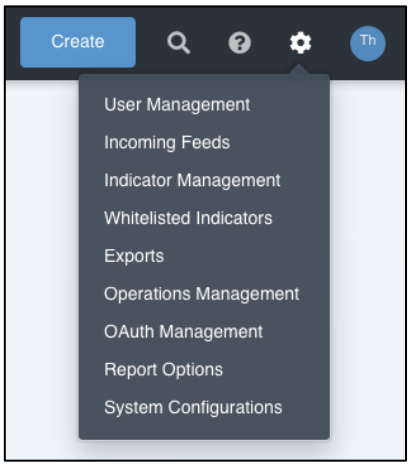
Installation or Upgrade is now complete.

1.6 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for Tenable.io Operation.

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

Figure 5: Operations Management – Configuration



2. Expand the **Operations Settings** configuration.

Figure 6: Operation Configuration

3. Input your **Access Key**: Your Tenable.io Access Key associated with your account.
4. Input your **Secret Key:** Your Tenable.io Secret Key associated with your account.
5. Click **Save Changes**.

   The operation is now ready to use.

1.7 Using the Operation

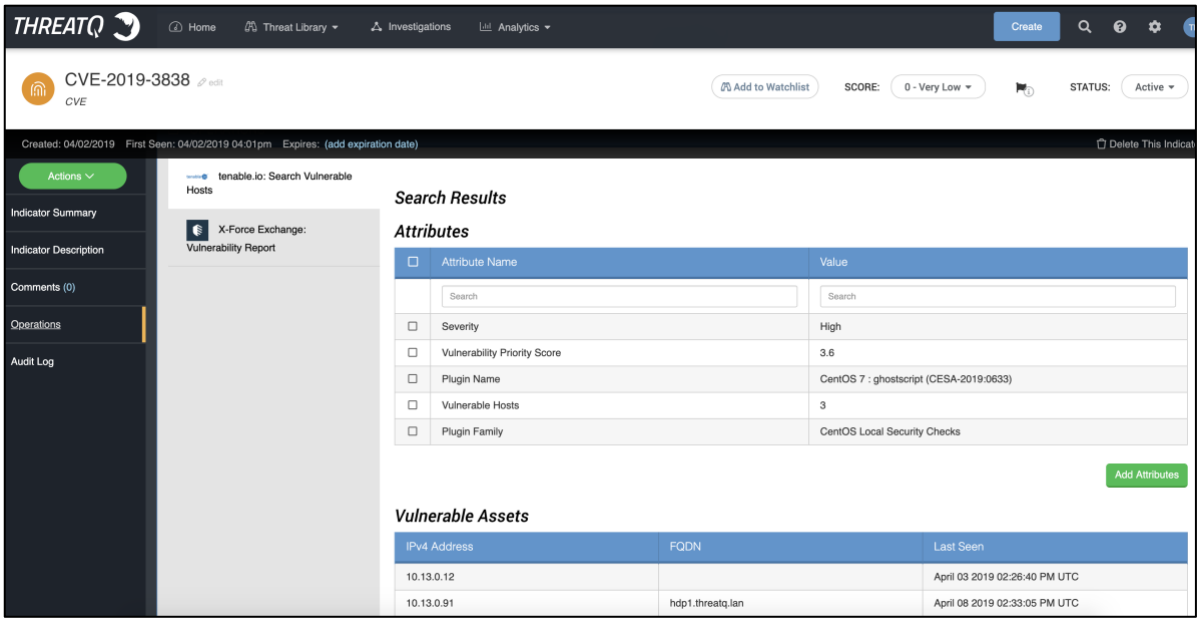
The following section covers the use of the ThreatQuotient for Tenable.io Operation.

Once the operation has been installed, navigate back to **Indicators** in the ThreatQ Threat Library.

1. Search for a CVE (e.g. CVE-2018-17972),
2. Click on the link. Scroll down to the Operations section of the indicator, and submit the operation by clicking on the **Tenable.io** button on the left.

This action will connect to the Tenable cloud instance, and will search the scan reports for hosts found to be vulnerable for the specific CVE. If any hosts are found, they will be listed in the ThreatQ UI. If none are vulnerable, the operation will return an empty JSON.

Figure 7: Operation Use



Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING 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 TERMS AND CONDITIONS WHEN PURCHASED. 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.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

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.