ThreatQuotient for QRadar Operation

January 22, 2019

Version 1.2.0

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 QRadar Operation provides a historical look up of events related to IP Address, FQDN, and URL type Indicators.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for QRadar 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 QRadar Operation	1.2.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for QRadar Operation into the managed estate:

- All ThreatQuotient equipment is online and in service.
- Infrastructure/transmission at all sites and between sites is in place to support the network traffic.
- All required firewall ports have been opened.
- All equipment is powered from permanent power supplies.
- A clock source of sufficient accuracy is connected to the network and the network and devices are using it as the primary clock source.

Implementation Overview

This document will give direction on how to install and configure the ThreatQuotient for QRadar Operation into the ThreatQ instance.

1.6 Prerequisites

You must have a valid QRadar Authorization Token. You can generate an Auth Token in the QRadar UI by navigating **Admin > Authorized Services > Add Authorized Services**.

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time (UTC recommended), time zone and date, and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

1.7 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.

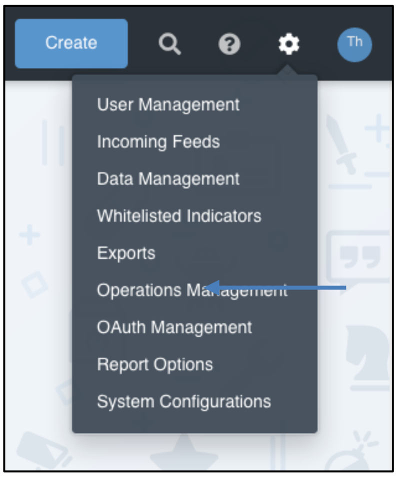
The data held within this document is classed as confidential due to its nature.

1.8 Setting up the Integration

Ensure the file `tq_qradar-1.2.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for QRadar Operation is being installed or upgraded.

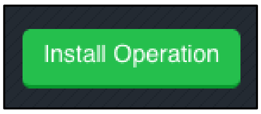
1. Navigate to **Settings** > **Operations Management**.

Figure 3: Operations Management – Install



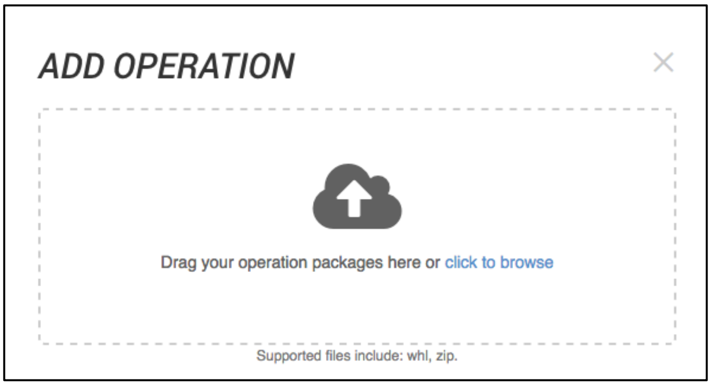
2. Click **Install Operation** in the upper right corner.

Figure 4: Install Operation



3. Drag the `tq_qradar-1.2.0-py3-none-any.whl` to the Add Operation dialog box or **click to browse** and to the required file.

Figure 5: Add Operation


ADD OPERATION

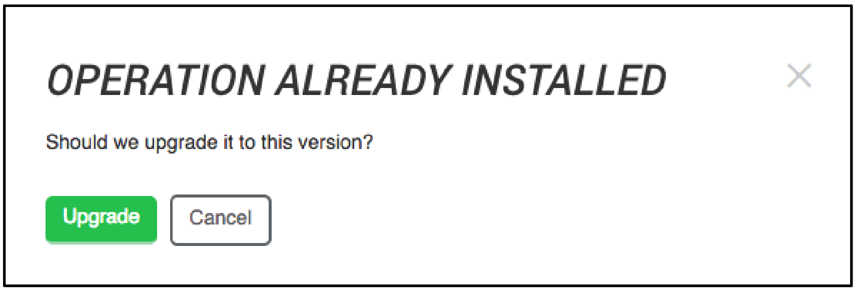
Drag your operation packages here or click to browse

Supported files include: whl, zip.

4. Click **Install** or **Upgrade**.

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

Figure 6: Upgrade Operation



OPERATION ALREADY INSTALLED

Should we upgrade it to this version?

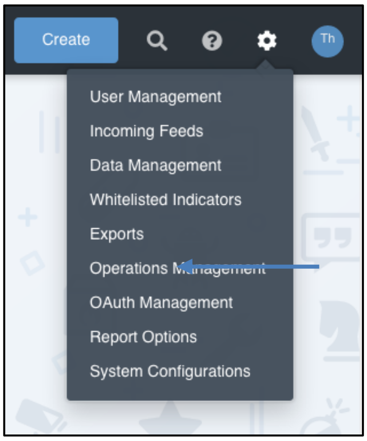
Installation / Upgrade is now complete.

1.9 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for QRadar Operation.

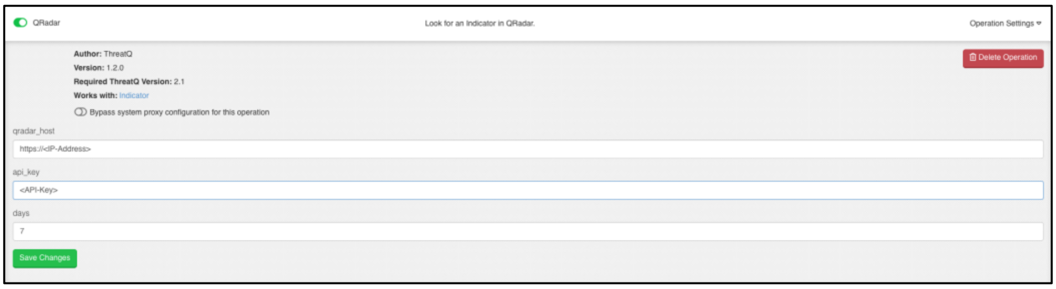
1. Navigate to **Settings** > **Operations Management.**

Figure 7: Operations Management – Configuration



2. Expand the **QRadar** configuration.

Figure 8: Operation Configuration



QRadar

Look for an Indicator in QRadar.

Author: ThreatQ
Version: 1.2.0
Required ThreatQ Version: 2.1
Works with: Indicator

○ Bypass system proxy configuration for this operation

qradar_host

https://<IP-Address>

api_key

<API-Key>

days

7

3. Input the Authorization Token from QRadar into the **API Key** field.
4. Click **Save Change**.
5. Click the toggle next to the **QRadar** name to enable the operation.

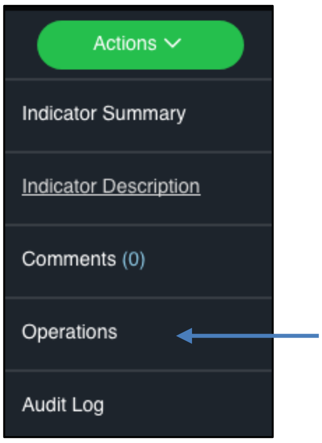
1.10 Running the Operation

The following section covers the practical use of the ThreatQuotient for QRadar Operation. The operation now includes the lookup of

- IP Addresses
- FQDN's,
- URL's

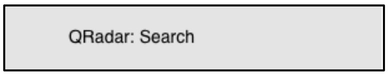
1. Navigate to an Indicator for look up**.**
2. Navigate to **Operations** on the Actions menus item on the left of the screen.

Figure 9: Operations Management – Configuration



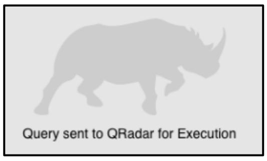
3. Click **QRadar: Search** only once to run the operation.

Figure 10: Operation Run 1st Click



When clicked, the operation will run the query against QRadar.

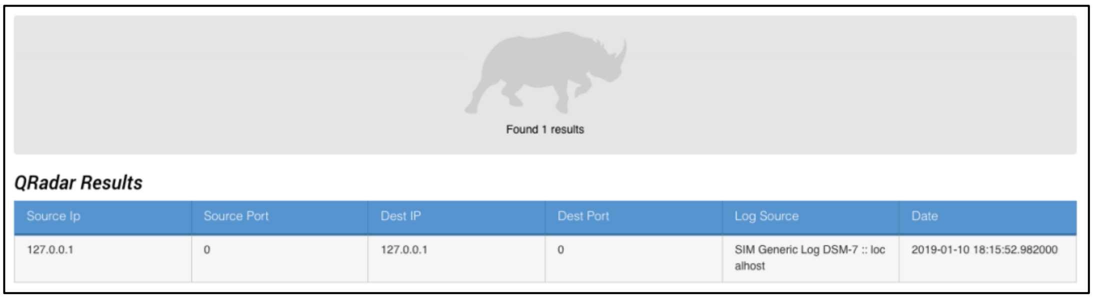
Figure 11: Operation Running



Query sent to QRadar for Execution

4. Click **QRadar: Search** a second time.

Figure 12: Operation Results



Found 1 results

QRadar Results

Source Ip	Source Port	Dest IP	Dest Port	Log Source	Date
127.0.0.1	0	127.0.0.1	0	SIM Generic Log DSM-7 :: loc alhost	2019-01-10 18:15:52.982000

The operation will return results from QRadar. *If IoC is in QRadar.

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.