ThreatQuotient for DomainTools Operation

June 5, 2018

Version 1.1.0

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

About This ThreatQuotient for DomainTools Operation

Author ThreatQuotient Professional Services

Document Conventions

Alerts readers to take note. Notes contain suggestions or references to material not covered in the document.

Alerts readers to be careful. In this situation, you may do something that could result in equipment damage or loss of data.

Alerts the reader that they could save time by performing the action described in the paragraph.

Alerts the reader that the information could help them solve a problem. The information might not be troubleshooting or even an action.

Introduction

Application Function

The ThreatQuotient for DomainTools Operation provides context in the form of attributes and indicators of compromise from the DomainTools API.

Preface

This guide provides the information necessary to implement the ThreatQuotient for DomainTools 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.

Audience

This document is intended for use by the following parties:

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

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 DomainTools Operation	1.1.0	

Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for DomainTools 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 provides direction for installing and configuring the ThreatQuotient for DomainTools Operation found within the ThreatQ instance.

Prerequisites

 You must have a valid DomainTools API Key.

Throughout this implementation document, there will be referrals 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, time zone and date, and using a clock source available to all.

For Example:

Figure 1: Time Zone Change Example

```
sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

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.

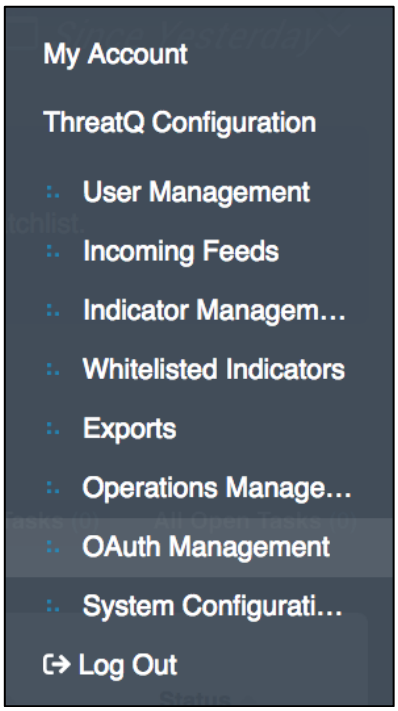
ThreatQuotient for DomainTools Operation Installation

Setting up the Integration

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

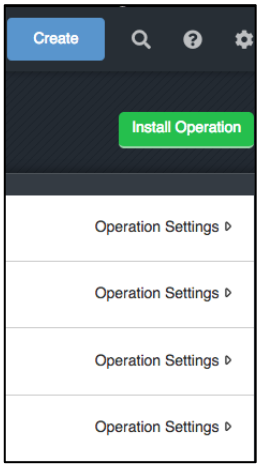
1. Navigate to **Settings** → **Operations Management**.

Figure 2: Operations Management – Install



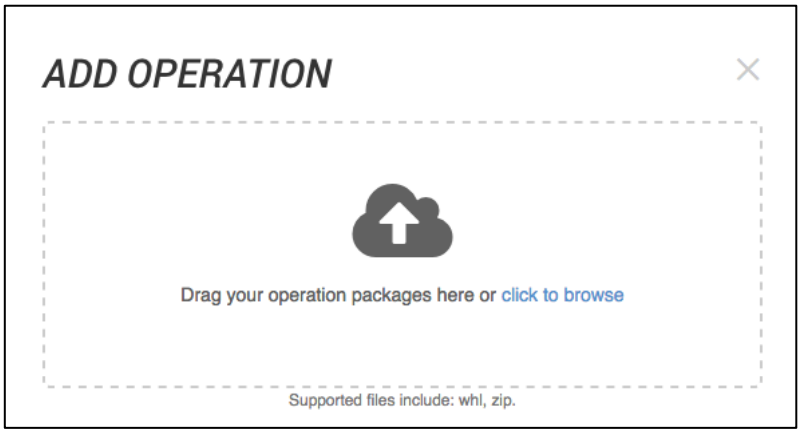
2. Click on the **Install Operation** button in the upper right corner.

Figure 3: Install Operation



3. Drag the `domaintools_WHOIS_parsed-X.X.X-py3-none-any.whl` to the Add Operation Popup or click to Browse and browse to the required file.

Figure 4: Add Operation



4. Click on the install / upgrade button.

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

Figure 5: Add Operation

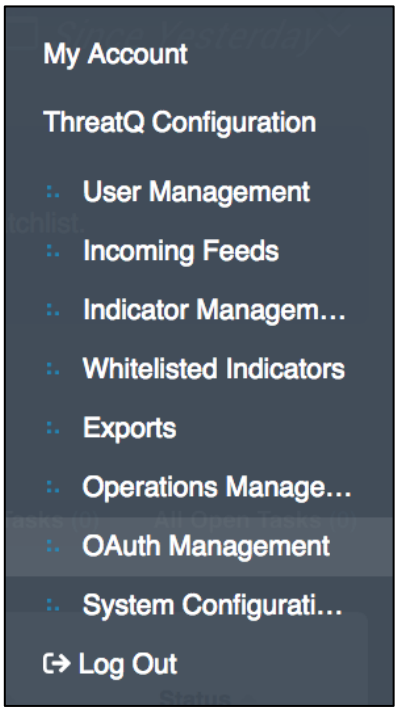
Installation / Upgrade is now complete.

Configuring the Operation

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

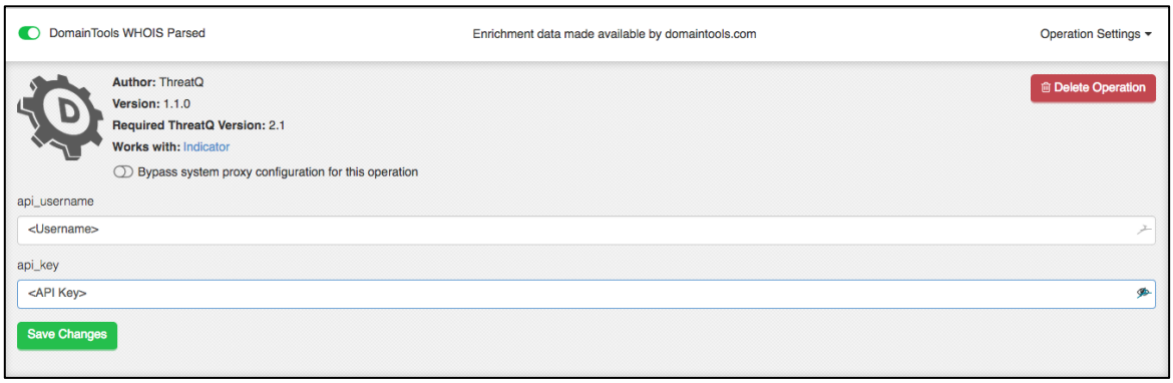
1. Navigate to **Settings** → **Operations Management.**

Figure 6: Operations Management – Configuration



2. Expand the **DomainTools WHOIS Parsed** configuration.

Figure 7: Operation Configuration



3. Input the API Username from DomainTools into the **api_username** field.
4. Input the API Key from DomainTools into the **api_key** field.
5. Click **Save Change**.
6. Click the toggle in next to the **DomainTools Whois Parsed** name to enable the operation.

Actions

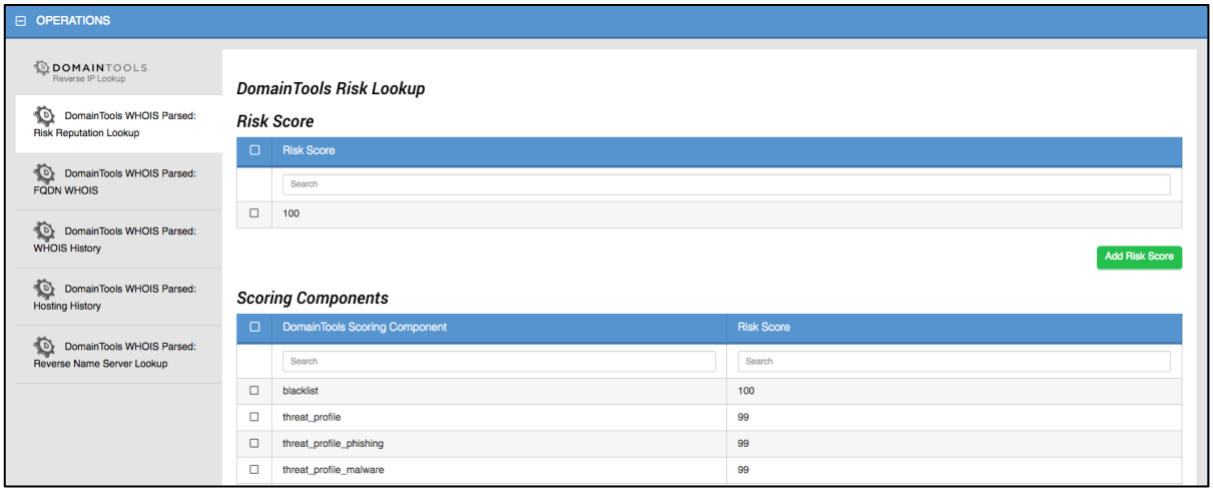
Table 2: Operation Actions Information

Action	Indicator Types	Description
IP Address WHOIS	IP Address	WHOIS information for an IP including network CIDR Blocks, registrant, ASN, and more
FQDN Address WHOIS	FQDN	WHOIS Information for an FQDN including related name servers, email addresses, registrant, and more
Reverse IP Lookup	IP Address, FQDN	Gets related IP Addresses for FQDN and related domains for IP Addresses
FQDN Address WHOIS History	FQDN	Enriches FQDNs with information from DomainTools WHOIS History so it can be determined if an FQDN is still a threat and how it has changed throughout time
Reverse Name Server Lookup	FQDN	Shows the primary and secondary domains hosted by the Name Server hosting this FQDN
Hosting History Lookup	FQDN	Enriches FQDNs with information from DT Hosting History *so that I* can understand the changes to the hosting for a specific FQDN

WHOIS

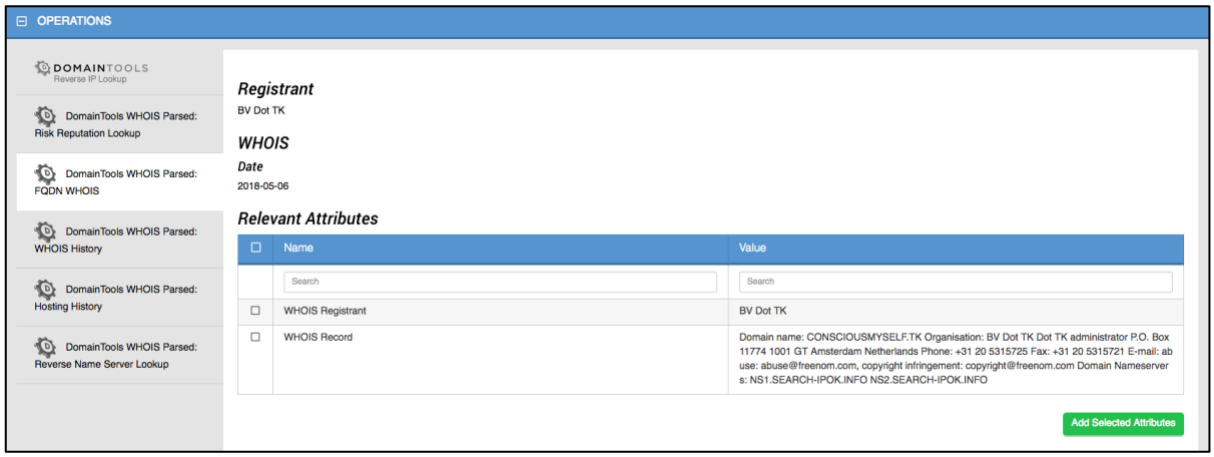
Risk Repudiation

Figure 8: WHOIS Risk Reputation Lookup



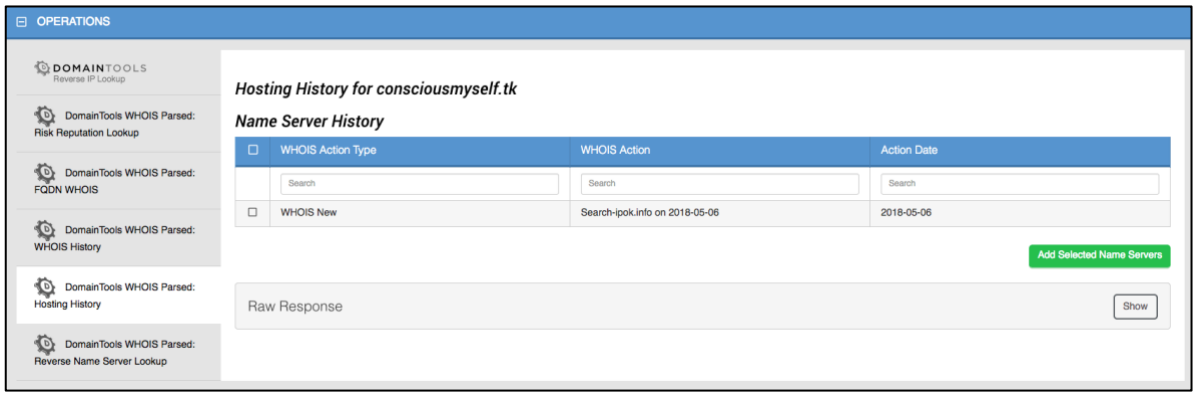
FQDN

Figure 9: WHOIS Operation FQDN



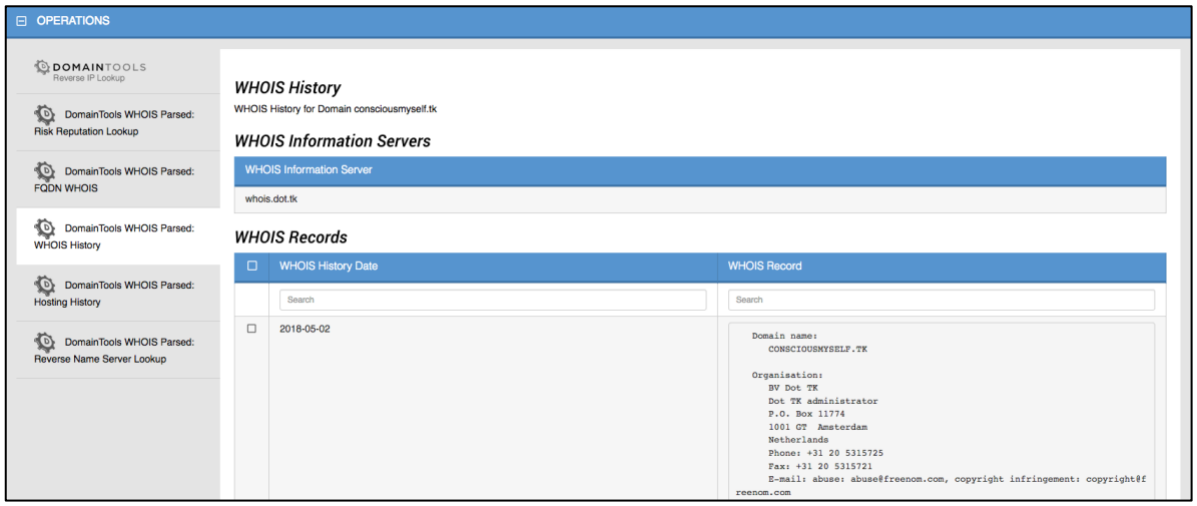
Hosting History Lookup

Figure 10: WHOIS Hosting History Lookup



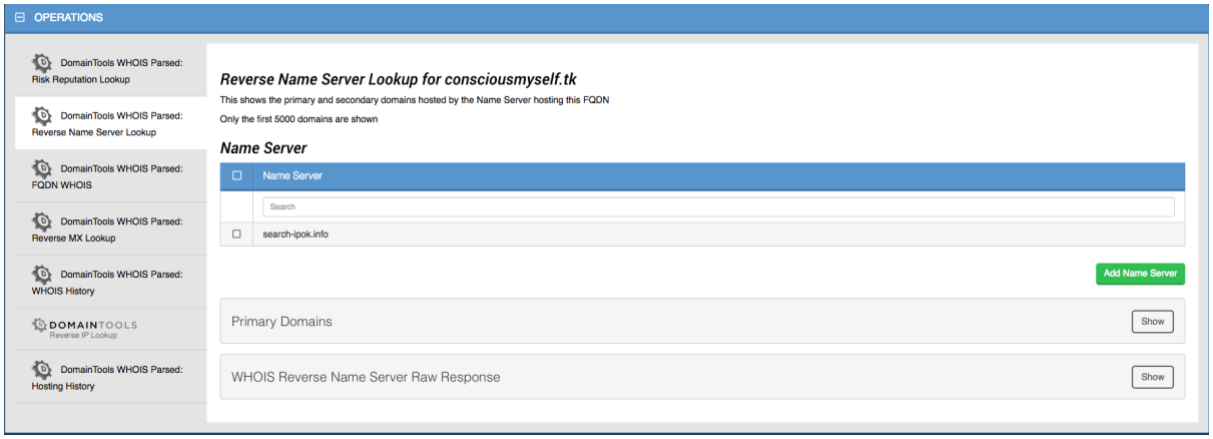
WHOIS History Lookup

Figure 11: WHOIS History



Reverse Name Server Lookup

Figure 12: WHOIS Reverse Name Server Lookup



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.