ThreatQuotient

Infoblox Dossier Operation Guide

Version 1.0.0

Tuesday, January 5, 2021

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: 4.40.0 or greater

Introduction

The ThreatQuotient for Infoblox Dossier Operation enables a ThreatQ user to query Infoblox Dossier for enrichment metadata.

Preface

This guide provides the information necessary to implement the ThreatQuotient for Infoblox Dossier 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.

Audience

This document is intended for use by the following parties:

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

Installation

Perform the following steps to install the integration:

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

1. Ensure the .whl file is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for Infoblox Dossier Operation is being installed/upgraded.
2. Navigate to the integrations management page on your ThreatQ instance.
3. Click on the **Add New Integration** button.
4. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

Note: *ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.*

You will still need to configure and then 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 integration-related credentials.*

To configure the operation:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operations** option from the Type dropdown (optional).

   Note: *If you are installing the integration for the first time, it will be located under the Disabled tab.*
3. Click on the operation to open its details page.
4. Enter the following configuration parameters:

Parameter	Description
API Key	API key for connecting to Infoblox Dossier.
Hostname	Hostname or IP address of Infoblox Dossier.
Port	Communication port (default is 8000).
Verify SSL	Check this box to verify SSL when connecting to the Infoblox Dossier instance.

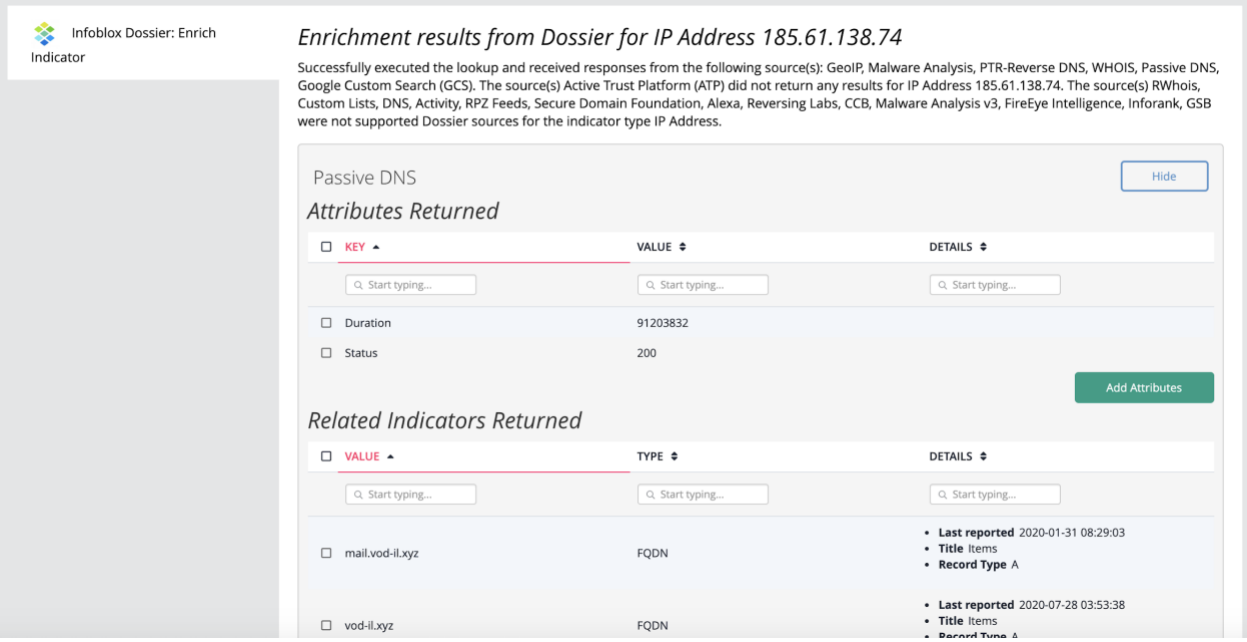
5. Click on **Save**.
6. Click on the toggle switch, located above the Additional Information section, to enable it.

Usasge

The operation can be executed on the following ThreatQ objects: IP Address, FQDN, URL, Email Address, MD5, SHA-1, and SHA-256. The operation supports different filters:

Object Type	Action	Filters Supported
Indicator	Search for Enrichment Data	Source

If the operation finds any enriching data, it will bring the following results back into the ThreatQ UI.



Change Log

Version	Details
1.0.0	Initial Release