

ThreatQuotient



DomainTools Operation Implementation Guide

Version 2.1.0

Friday, October 11, 2019

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.

Copyright © 2019 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Friday, October 11, 2019

Contents

DomainTools Operation Implementation Guide	1
Warning and Disclaimer	2
Contents	4
Versioning	5
Introduction	6
Requirements	6
Installation	6
Configuration	6
Actions	7
Advanced Configuration	7
WHOIS Parsed	9
IRIS Investigate	11
Domain Reputation	12
Hosting History	13
Reverse IP	14
Reverse Whois	15

Versioning

- Current integration version: 2.1.0
- Supported on ThreatQ versions: 4.24.0 or higher

Introduction

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

Requirements

The DomainTools Operation requires a **DomainTools API Key** from the vendor before it can be enabled in ThreatQ.

Installation

ThreatQ v4.24.0 and above includes the DomainTools Operation v2.1.0 by default and overwrites version 0.0.3 that was installed with the platform.



If you have manually installed any other version of Domain Tools, ThreatQ will retain that version along with v2.1.0.

Configuration

To configure the DomainTools operation:

1. From the ThreatQ user interface, select the **Settings icon > Operations Management**.
2. Expand the **DomainTools** configuration.
3. For **api_username**, enter the API Username from DomainTools.

4. For **api_key**, enter the API Key from DomainTools.
5. Click **Save Changes**.
6. Click the toggle next to **DomainTools** to enable.

Actions

Action	Indicator Types	Description
Enrichment	IP Address and FQDNs	Information for IP addresses and FQDNs, including registrant, name servers, email addresses, and more. The operation has been updated to include the latest endpoints.

Advanced Configuration

The endpoints you can call for enrichment are configurable as displayed below:

Operation: Domain Tools



IRIS API

The Iris Investigate API is suited for investigate and orchestrate uses cases at human scale.

☐ IRIS Investigate

Provides dozens of domain name attributes for indicators

ENTERPRISE API

Provides basic details data for domain and IP address indicators

☐ WHOIS Parsed

Parsed results for Whois records for domain names and IP addresses

☐ Reputation Lookup

Provides risk score information for domains

☐ Hosting History

Provides the changes that have occurred in a domain names registrar, IP address, and name servers

☐ Reverse IP

Provides a list of domain names that share the same Internet host

Run

Cancel

WHOIS Parsed

WHOIS Parsed enriches data with parsed results for Whois records for domain names and IP addresses. The url that is called is <https://api.domaintools.com/v1/{}/whois/parsed> and the mapping consists of:

Domain Tools	TQ Name	TQ Type	Example
registrant	Registrant	Indicator Attribute	DomainTools, LLC
registrant_email	Registrant Email	Indicator Attribute	
created_date	Created At	Indicator Attribute	
updated_date	Updated At	Indicator Attribute	
statuses	Status	Indicator Attribute	
networks[].range.from.value	IP	Related Indicator	
networks[].range.to.value	IP	Related Indicator	

Domain Tools	TQ Name	TQ Type	Example
networks[].range.cidr[].value	CIDR BLOCK	Related Indicator	
response.parsed_whois.networks[].name	WHOIS Name	Indicator Attribute	
response.parsed_whois.networks[].organization	WHOIS Organization	Indicator Attribute	
response.parsed_whois.routes[].id	CIDR Block	Related Indicator	
response.parsed_whois.routes[].asn[].value	ASN	Attribute	
response.parsed_whois.referral_servers[].value	FQDN	Related Indicator	
source	Source	Indicator Attribute	
country	Country	Indicator Attribute	
contacts	Phone	Indicator Attribute	
status	Status	Indicator Attribute	

Domain Tools	TQ Name	TQ Type	Example
ref	References	Indicator Attribute	
record_source	Record Source	Indicator Attribute	

IRIS Investigate

IRIS Investigate provides dozens of domain name attributes for indicators. Based on the indicator type, the URL called is either <https://api.domaintools.com/v1/iris-investigate/?ip={ }> or <https://api.domaintools.com/v1/iris-investigate/?domain={ }> and the mapping consists of:

Domain Tools	ThreatQ Name	ThreatQ Type	Example
whois_url	WHOIS URL	Indicator Attribute	https://whois.domaintools.com/desitales.com
admin_contact	Admin	Indicator Attribute	
email_domain[]	email domain	Related Indicator	
registrant_contact	All Regis- trant Data	Attribute	
billing_contact	All Billing Data	Attribute	

Domain Tools	ThreatQ Name	ThreatQ Type	Example
create_date	Created At	Attribute	
expiration_date	Expiration Date	Attribute	
ssl_email	SSL email	Attribute	
ip[]	All address data	Related Indicator	
domain_risk.-component [].name / domain_risk.-component [].risk_score	Domain Risk Name and Score	Attribute	

Domain Reputation

Reputation Lookup provides risk score information for domains. The endpoint URL is https://api.domaintools.com/v1/reputation/?domain={}&include_reasons=true and the mapping consists of:

Domain Tools	ThreatQ Name	ThreatQ Type	Example
risk_score	Risk Score	Indicator Attribute	21.13

Domain Tools	ThreatQ Name	ThreatQ Type	Example
response.reasons[]	Scoring Reason	Indicator Attribute registrant	

Hosting History

Hosting History provides the changes that have occurred in a domain name's registrar, IP address, and name servers. The endpoint URL is <https://api.domaintools.com/v1/{}/hosting-history/> and the mapping consists of:

DomainTools	ThreatQ Name	ThreatQ Type	Example
registrar_history [].registrar	WHOIS Registrar	Indicator Attribute	
registrar_history [].date_updated	Updated At	Indicator Attribute	
nameserver_history[].pre_mns	FQDN	Indicator Value	
nameserver_history[].post_mns	FQDN	Indicator Value	
nameserver_history[].action_in_words	WHOIS Action	Attribute Value	Transfer

DomainTools	ThreatQ Name	ThreatQ Type	Example
nameserver_history[].actiondate	WHOIS Action Date	Attribute Value	
ip_history[].post_ip	Indicator Value	IP Address	
ip_history[].pre_ip	Indicator Value	IP Address	
ip_history[].action_in_words	WHOIS Action	Attribute Value	
ip_history[].actiondate	WHOIS ActionDate	Attribute Value	

Reverse IP

Reverse IP provides a list of domain names that share the same Internet host. If the indicator is an FQDN, the called endpoint will be: <https://api.domaintools.com/v1/{fqdn}/reverse-ip/>, otherwise <https://api.domaintools.com/v1/{ip}/host-domains/> and the mapping will be the following:

Domain Tools	ThreatQ Name	ThreatQ Type	Example
ip_address	IP Address	Indicator Value	199.30.228.112

If the indicator is an IP, the called endpoint will be: <https://api.domaintools.com/v1/{ip}/host-domains/> and the mapping will be the following:

Domain Tools	ThreatQ Name	ThreatQ Type	Example
ip_address	IP Address	Indicator Value	199.30.228.112
domain_names[]	FQDN	Indicator Value	

Reverse Whois

Reverse Whois allows search for domains by the name, address, telephone number, email address or physical address of the Registrant listed. The endpoint URL is <http://api.domaintools.com/v1/reverse-whois/?terms={email}&mode=purchase> and the mapping consists of:

Domain Tools	ThreatQ Name	ThreatQ Type	Example
domains	Domain Name	Domain Name	bulkcheck.com