

ThreatQuotient



ThreatQ ACE Operation Guide

Version 1.0.0

February 14, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Integration Details	5
Introduction	6
Prerequisites	7
ThreatQ ACE Library	7
Installation	8
Configuration	9
Actions	10
Parse	11
Parse Parameters	11
Example - Parsed Tags	13
Example - Parsed Attributes	14
Example - Parsed Adversaries	15
Example - Parsed Malware	16
Example - Parsed Indicators	17
Example - Parsed Vulnerabilities	18
Example - Parsed MITRE ATT&CK Techniques	19
Change Log	20

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 © 2023 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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
-----------------------------	-------

Compatible with ThreatQ Versions	>= 4.35.0
----------------------------------	-----------

Support Tier	ThreatQ Supported
--------------	-------------------

ThreatQ Marketplace	https:// marketplace.threatq.com/ details/threatq-ace- operation
---------------------	--

Introduction

The ThreatQ ACE operation utilizes the ThreatQ ACE library for parsing unstructured text for contextual intelligence such as IOCs, malware, adversaries, and tags.

The operation provides the following action:

- **Parse** - parses a selected object's unstructured description text for contextualization.

The operation is compatible with the following system objects:

- Adversaries
- Campaigns
- Events
- Files
- Incidents
- Malware
- Reports

Prerequisites

The ThreatQ ACE operation requires the installation of the ThreatQ ACE Library. This library must be installed prior to attempting to install the operation. Failure to do so will result in the operation installation process failing.

ThreatQ ACE Library

The required ThreatQ ACE library is included in the operation's marketplace download. Use the following steps to install the library.

 When installing the library, be aware that any in-progress feed runs will be cancelled when initiating step 6.

1. Locate the **threatq_ace-<version>-py3-none-any.whl** library file bundled with the operation file.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

```
<> cd /tmp/
```

4. Upload the library file to this directory.
5. Install the library:

```
<> sudo -u apache /opt/threatq/python/bin/pip install  
threatq_ace-<version>-py3-none-any.whl
```

6. Restart Dynamo:

```
<> systemctl restart threatq-dynamo
```

7. Proceed with [installing the operation](#).

Installation



The operation requires the installation of the ThreatQ ACE library prior to installing the operation. See the [Prerequisites](#) section for more details.

Perform the following steps to install the integration:



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

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. 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



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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure and then enable](#) the operation.

Configuration



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 integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Parse	Parses the given object for context.	Adversary, Campaign, Incident, Event, File, Malware, Report	N/A

Parse

The Parse action parses the selected object's unstructured description text for contextualization.

Parse Parameters

The Parse action provides the following configuration parameters:

PARAMETER	DESCRIPTION
Dry Run	Disable this option to have the operation automatically upload the parsed context to the ThreatQ platform.
Select Parsers	Select which parsers to use in extract data from the current object. Options include: • Indicators (default) • Vulnerabilities • Attributes • Tags • Malware • Adversaries • Attack Patterns
Parsed IOC Types	Select which IOCs types to parse for with the operation. Options include: • MD5 (default) • SHA-1 (default) • SHA-256 (default) • SHA-384 • CIDR Block (default) • URL (default) • FQDN (default) • Email Address • IP Address (default) • Filename • File Path
Default IOC Status	Select the default status of IOCs that are automatically ingested into the platform. This option only applies when you are have disabled the Dry Run option.

Configuration Parameters

☒ Dry Run

If disabled, this action will automatically upload the parsed context to ThreatQ. Indicators will be added with the "Review" status.

Select Parsers

Select which parsers to use to extract data from the current object

- ☒ Indicators
- ☐ Vulnerabilities
- ☐ Attributes
- ☐ Tags
- ☐ Malware
- ☐ Adversaries
- ☐ Attack Patterns

Parsed IOC Types

Select which IOC types to parse for

- ☒ MD5
- ☒ SHA-1
- ☒ SHA-256
- ☐ SHA-384
- ☒ CIDR Block
- ☒ URL
- ☒ FQDN
- ☐ Email Address
- ☒ IP Address
- ☐ Filename
- ☐ File Path

Default IOC Status

Review

Select the default status for IOCs automatically ingested into ThreatQ (when dry run is disabled)

Example - Parsed Tags

Parsed Tags (Time: 0.061)

☐ NAME ⇅

Search 10 reco

☐ tlp:white

☐ exploit

☐ C2

☐ malware

☐ apt

☐ breach

☐ vulnerability

☐ exfiltration

☐ PII

☐ spoofing

Example - Parsed Attributes

Parsed Attributes (Time: 0.239)

NAME		VALUE	
Search 40 reco		Search 40 reco	
☐	Affected Operating System		Windows
☐	Affected Operating System		Linux
☐	Detection		Trojan.PHP.Shell.JB
☐	Detection		Trojan.Script.Crypt.dsonvo
☐	Detection		Trojan.PHP.Crypt
☐	Detection		Trojan.PHP.Shell.LV
☐	Detection		Trojan.Win32.Malware
☐	Detection		W32/Trojan3.XZP
☐	Detection		Trojan.Generic.20173242
☐	Detection		Trojan.Cozer.B
☐	Detection		Win.Trojan.OnionDuke-5486244-0
☐	Detection		Trojan.Win32.MiniDuke.ekecow
☐	Detection		W32/Trojan3.XZO
☐	Detection		Trojan.Generic.20173160
☐	Detection		Win.Trojan.OnionDuke-5486245-0
☐	Detection		Trojan.Win32.AD.ekdqnf
☐	Detection		Trojan.Win32.Agent
☐	Detection		W32/Dridex.HX
☐	Detection		Win.Trojan.Agent-5486255-0
☐	Detection		Trojan.Rtf.Stealer.efqzyl
☐	Detection		Trojan.Win32.Zlader
☐	Detection		Trojan.Win32.Crypt5.AYWX
☐	Detection		Trojan.Fareit.Win32.14782
☐	Detection		Win.Trojan.Agent-5486256-0
☐	Detection		Trojan/Win32.Fareit

< 1 2 > | Rows per page 25

Add Selected Attributes

Example - Parsed Adversaries

Parsed Adversaries (Time: 0.955)

☐
NAME

Search 5 records

☐	APT28
☐	APT29
☐	GRIZZLY STEPPE
☐	Voodoo Bear
☐	Threat Group-4127

Example - Parsed Malware

Parsed Malware (Time: 2.252)

☐

VALUE

⌵

☐	APT28
--------------------------	-------

Example - Parsed Indicators

Parsed Indicators (Time: 0.21)

☐ VALUE	☐ TYPE
Search 318 rec	Search 318 rec
☐ g.boot.txt.rar.msi.zip	FQDN
☐ private.directinvesting.com	FQDN
☐ cderlearn.com	FQDN
☐ wilcarobbe.com	FQDN
☐ one2shoppee.com	FQDN
☐ ritsoperrol.ru	FQDN
☐ littjohnwillhap.ru	FQDN
☐ insta.reduct.ru	FQDN
☐ editprod.waterfilter.in.ua	FQDN
☐ mymodule.waterfilter.in.ua	FQDN
☐ Trojan.PHP.Shell.LV	FQDN
☐ Backdoor.PHP.Agent.abb	FQDN
☐ Backdoor.Win32.MiniDuke.bz	FQDN
☐ Trojan.Win32.AD	FQDN
☐ cderlearn.com	FQDN
☐ Trojan.W1n32.AD	FQDN
☐ waterfilter.in.ua	FQDN
☐ directinvesting.com	FQDN
☐ whois.networksolutions.com	FQDN
☐ NS1.LNHI.NET	FQDN
☐ NS2.LNHI.NET	FQDN
☐ NS3.LNHI.NET	FQDN
☐ mail.moneypaper.com	FQDN
☐ NS1.WESTSERVERS.NET	FQDN
☐ NS2.WESTSERVERS.NET	FQDN

< **1** 2 3 4 5 6 7 ... 13 > | Rows per page 25 ▾

Add Selected Indicators

Example - Parsed Vulnerabilities

Parsed Vulnerabilities (Time: 0.21)

VALUE

TYPE

Search 10 reco

Search 10 reco

☐	CVE-2016-7855	CVE
☐	CVE-2016-7255	CVE
☐	CVE-2016-4117	CVE
☐	CVE-2015-1641	CVE
☐	CVE-2015-2424	CVE
☐	CVE-2014-1761	CVE
☐	CVE-2013-2729	CVE
☐	CVE-2012-0158	CVE
☐	CVE-2010-3333	CVE
☐	CVE-2009-3129	CVE

Add Selected Indicators

ThreatQ ACE Operation Guide

Version 1.0.0

18

Example - Parsed MITRE ATT&CK Techniques

Parsed MITRE ATT&CK Techniques (Time: 0.897)

No data was found

0

Unstructured Text

Show

Raw Response

Show

Change Log

- Version 1.0.0
 - Initial release