

ThreatQuotient



ThreatQuotient for Lastline Operation

Version 2.0.0

April 26, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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: Wednesday, April 26, 2019

Contents

WARNING AND DISCLAIMER.....	2
CONTENTS	4
LIST OF FIGURES AND TABLES	5
INTRODUCTION	6
1.1 APPLICATION FUNCTION	6
1.2 PREFACE	6
1.3 AUDIENCE	6
1.4 SCOPE	6
THREATQUOTIENT FOR LASTLINE OPERATION INSTALLATION	7
1.5 SETTING UP THE INTEGRATION	7
1.6 CONFIGURING THE OPERATION	9
1.7 USING THE OPERATION	10
TRADEMARKS AND DISCLAIMERS	15

List of Figures and Tables

FIGURE 1: OPERATIONS MANAGEMENT – INSTALL	7
FIGURE 2: INSTALL OPERATION	7
FIGURE 3: ADD OPERATION	8
FIGURE 4: ADD OPERATION	8
FIGURE 5: OPERATIONS MANAGEMENT – CONFIGURATION	9
FIGURE 6: OPERATION CONFIGURATION.....	9
FIGURE 7: OPERATION SUBMIT	10
FIGURE 7: OPERATION SUBMIT RESULTS SUCCESS.....	10
FIGURE 7: OPERATION GET REPORTS SUBMIT.....	11
FIGURE 7: OPERATION API CALLS EXAMPLE	11
FIGURE 7: OPERATION CODE HASHES ANALYSIS EXAMPLE	11
FIGURE 7: OPERATION MUTEX EXAMPLE.....	12
FIGURE 7: OPERATION NETWORK EXAMPLE.....	12
FIGURE 7: OPERATION PROCESS EXAMPLE.....	12
FIGURE 7: OPERATION OPENED WINDOW EXAMPLE	13
FIGURE 7: OPERATION QUERY PARAMETER EXAMPLE	13
FIGURE 7: OPERATION QUERY IP ADDRESS EXAMPLE	13
FIGURE 7: OPERATION QUERY DOMAIN EXAMPLE.....	14
FIGURE 7: OPERATION QUERY REPUTATION EXAMPLE	14
 TABLE 1: THREATQUOTIENT SOFTWARE & APP VERSION INFORMATION	 6

Introduction

1.1 Application Function

The ThreatQuotient for Lastline Operation allows ThreatQ users to query tasks and network reputations, as well as submit files, URLs, and domains, and retrieve task reports from Lastline.

1.2 Preface

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

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 Lastline Operation	2.0.0	

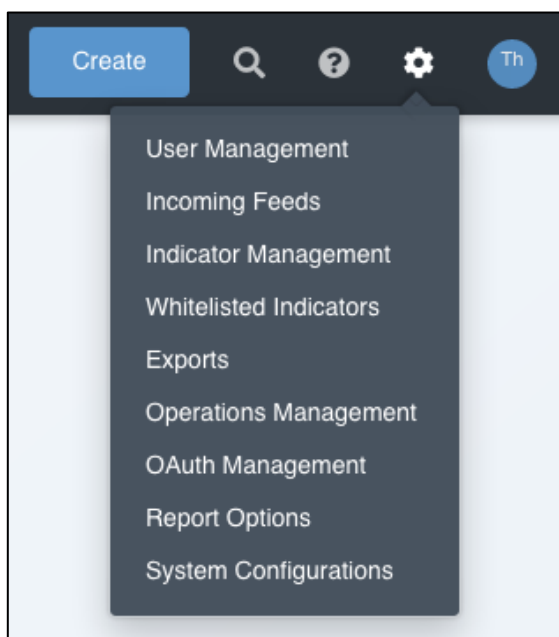
ThreatQuotient for Lastline Operation Installation

1.5 Setting up the Integration

Ensure the file `tq_op_lastline-2.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for Lastline Operation is being installed or upgraded.

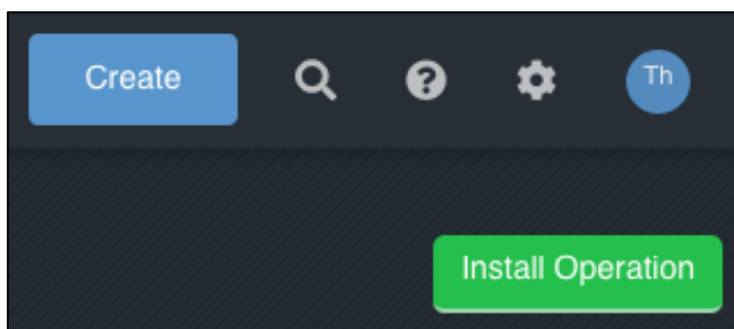
1. Navigate to the **Settings icon > Operations Management**.

Figure 1: Operations Management – Install



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

Figure 2: Install Operation



3. Drag the `tq_op_lastline-2.0.0-py3-none-any.whl` to the Add Operation Popup or **Click to Browse** to the required file.

Figure 3: Add Operation

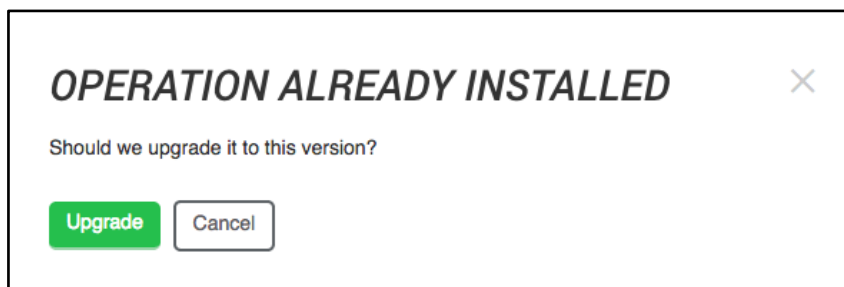


4. Click **Install** or **Upgrade**.



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

Figure 4: Add Operation



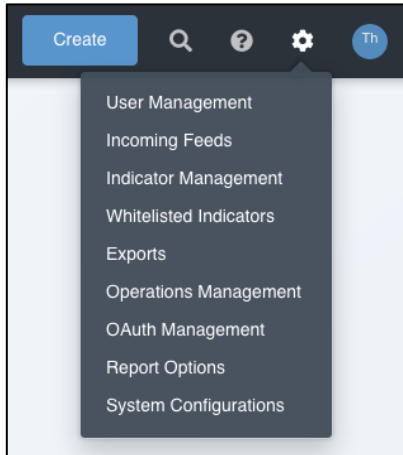
Installation or upgrade is now complete.

1.6 Configuring the Operation

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

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

Figure 5: Operations Management – Configuration



2. Expand the **Operations Settings** configuration.

Figure 6: Operation Configuration

A screenshot of the 'Operation Configuration' form in the ThreatQuotient application. The form is titled 'Author: ThreatQ Version: 2.0.0' and 'Required ThreatQ Version: 2.1'. It includes a checkbox for 'Works with: Attachment Indicator' and a note to 'Bypass system proxy configuration for this operation'. The form contains three input fields: 'lastline_api_host' (pre-filled with 'https://user.lastline.com/api'), 'lastline_username', and 'lastline_password'. A 'Save Changes' button is at the bottom left, and a 'Delete Operation' button is at the top right.

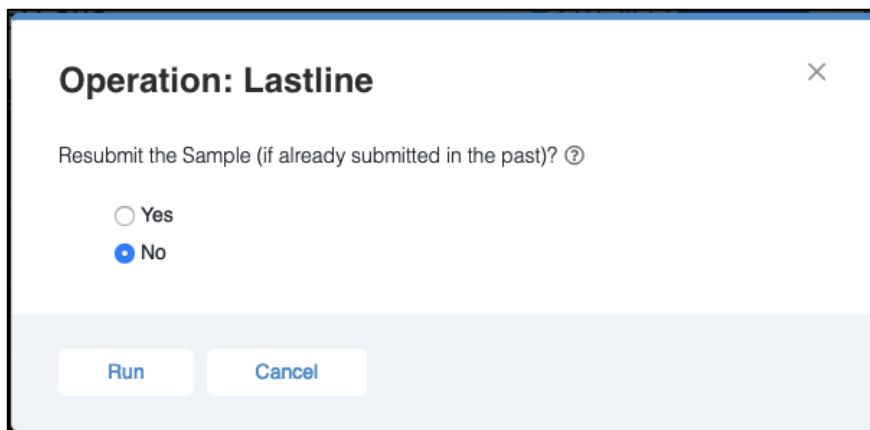
3. Input your **lastline_username**: Your Lastline username for the API.
4. Input your **lastline_password**: Your Lastline password for the API.

1.7 Using the Operation

The following section covers the use of the ThreatQuotient for Lastline Operation. This action will submit a file (attachment) or a URL/FQDN to Lastline Analyst for sandboxing.

1. Navigate to a suitable indicator found in ThreatQ that you want to scan.
2. Navigate to the **Operations** section on the left-hand side.
 - A Lastline entry will be available.
3. Click the Lastline entry to run the operation. You will be presented with a popup window asking for further information.
4. Once the operation has run, a result similar to the example below will display.

Figure 7: Operation Submit



Operation: Lastline [X]

Resubmit the Sample (if already submitted in the past)? ⓘ

☐ Yes

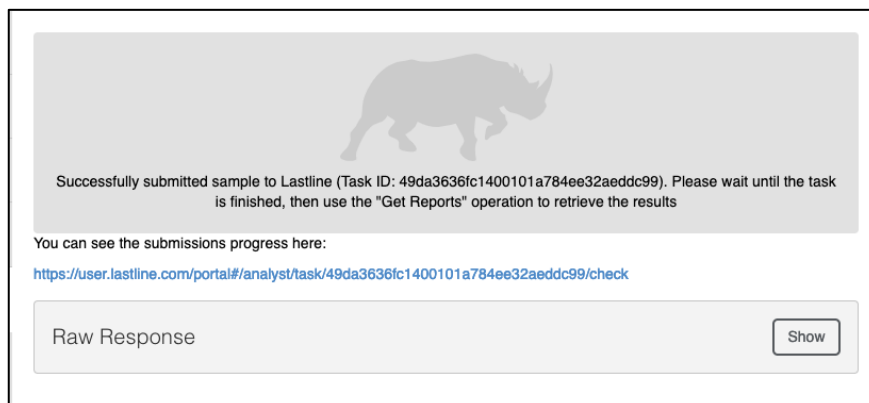
☒ No


Run **Cancel**

Resubmit the Sample

By default, the option is set to **No**. If a sample has already been submitted from ThreatQ, it will prevent the user from resubmitting the sample. If the sample needs to be resubmitted, it can be done by selecting **Yes** to override this.

Figure 8: Operation Submit Results Success





Successfully submitted sample to Lastline (Task ID: 49da3636fc1400101a784ee32aedd99). Please wait until the task is finished, then use the "Get Reports" operation to retrieve the results

You can see the submissions progress here:
<https://user.lastline.com/portal#/analyst/task/49da3636fc1400101a784ee32aedd99/check>

Raw Response **Show**

Get Reports

This action will retrieve all the reports for the sample, with the only condition being that the sample (in ThreatQ) has an attribute with the name "Lastline Task ID" and the value will be the task ID. For each of these attributes, it will fetch a report correlating to the submission ID. If submission results are found, results will be shown and the full JSON report will be uploaded and related to the sample in ThreatQ.

Figure 9: Operation Get Reports Submit

Task 49da3636c1400101a784ee32aed0c99

Successfully updated and related JSON report

Subject Indicators

Name	Type
<input type="checkbox"/> c8fda7a83a08b5c1376708705aee75a2025a6a4	SHA-1
<input type="checkbox"/> a89a50f0a281ac3f1c17a2b9a6c7832	MD5
<input type="checkbox"/> 4122554827442b6aee7287c7238710593a870818a0a847a6d5824148044a43	SHA-256

[Add Selected Indicators](#)

Report Overview

Showing 1 to 10 of 25

Name	Value
<input type="checkbox"/> Lastline Score	100
<input type="checkbox"/> Analysis Engine	LLama - WindowsXP
<input type="checkbox"/> Malicious Activity	Anomaly: Ability to check current user's privileges
<input type="checkbox"/> Malicious Activity	Anomaly: Identified potentially malicious code
<input type="checkbox"/> Malicious Activity	Anomaly: Potentially malicious application/program
<input type="checkbox"/> Malicious Activity	Autoshield: Registering a dll for automatic loading in user applications
<input type="checkbox"/> Malicious Activity	Autoshield: Registering a new service at startup
<input type="checkbox"/> Malicious Activity	Evasion: Possibly stalling against analysis environment (sleep)
<input type="checkbox"/> Malicious Activity	Execution: Ability to create service
<input type="checkbox"/> Malicious Activity	Execution: Ability to enumerate domains and user shares

[Previous](#) [Next](#) [Add Selected Attributes](#) [Show](#)

Analysis for subject 2

API calls Example

Figure 10: Operation API calls Example

API Call Info [Hide](#)

API Calls

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	Search	Search
<input type="checkbox"/>	API Call	NtClose
<input type="checkbox"/>	API Call	NtWaitForSingleObject
<input type="checkbox"/>	API Call	NtAllocateVirtualMemory
<input type="checkbox"/>	API Call	GetSystemMetrics

[Add Selected Attributes](#)

Code Hashes Analysis Example

Figure 11: Operation Code Hashes Analysis Example

Code Hash Analysis [Hide](#)

Threats

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	Search	Search
<input type="checkbox"/>	Threat Name	klez
<input type="checkbox"/>	Threat Class	worm
<input type="checkbox"/>	Threat Name	unknown
<input type="checkbox"/>	Threat Class	benign

[Add Selected Attributes](#)

Mutex Example

Figure 12: Operation Mutex Example

Mutexes		Hide
Mutex Indicators		
<input type="checkbox"/>	Value	Type
	Search	Search
<input type="checkbox"/>	CTF.Asm.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003	Mutex
<input type="checkbox"/>	CTF.Layouts.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003	Mutex
<input type="checkbox"/>	CTF.LBES.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003	Mutex
<input type="checkbox"/>	MSCTF.Shared.MUTEX.IDD	Mutex
<input type="checkbox"/>	CTF.TMD.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003	Mutex
<input type="checkbox"/>	MSCTF.Shared.MUTEX.MH	Mutex
<input type="checkbox"/>	CTF.TimListCache.FMPDefaultS-1-5-21-1229272821-1563985344-1801674531-1003MUTEX.DefaultS-1-5-21-1229272821-1563985344-1801674531-1003	Mutex
<input type="checkbox"/>	CTF.Compart.MutexDefaultS-1-5-21-1229272821-1563985344-1801674531-1003	Mutex
<input type="checkbox"/>	ShimCacheMutex	Mutex
Add Selected Indicators		

Network Indictors Example

Figure 13: Operation Network Example

Network Activity		Hide
Network Indicators		
Showing 1 to 10 of 110		Row count: 10
<input type="checkbox"/>	Value	Type
	Search	Search
<input type="checkbox"/>	thisgrown.net	FQDN
<input type="checkbox"/>	10.0.2.3	IP Address
<input type="checkbox"/>	elementarimagine.com	FQDN
<input type="checkbox"/>	gladword.net	FQDN
<input type="checkbox"/>	equaltouch.net	FQDN
<input type="checkbox"/>	salttouch.net	FQDN
<input type="checkbox"/>	salthave.net	FQDN
<input type="checkbox"/>	spokeblack.net	FQDN
<input type="checkbox"/>	dreamplain.net	FQDN
<input type="checkbox"/>	watchplain.net	FQDN
Previous		Next
Add Selected Indicators		

Process Example

Figure 14: Operation Process Example

Process Indicators

<input type="checkbox"/>	Value	Type
	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	file.exe	Filename
<input type="checkbox"/>	C:\DOCUME~1\Miller\LOCALS~1\Temp\file.exe	File Path
<input type="checkbox"/>	41220549274428abee7267d72987c00f3d970518cce8d47ee5c82d148bf44ae3	SHA-256
<input type="checkbox"/>	c25e5a7a62e0d65c137670670eae71b2503abe5	SHA-1
<input type="checkbox"/>	a99afd20a2a91ac3f1c17e0fb96c7832	MD5

Add Selected Indicators

Process Attributes

<input type="checkbox"/>	Name	Value
	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	YARA Signature Hit	ExtensionList

Add Selected Attributes

Opened Window Example

Figure 15: Operation Opened Window Example

Opened Windows

Hide

Window Information

<input type="checkbox"/>	Name	Value
	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	Invisible Window	False
<input type="checkbox"/>	Opened Window Title	[download in progress...] Kodak Viewer Express - Picture 1 of 1

Add Selected Attributes

Query Tasks

This action will allow you to query tasks within Lastline Knowledge base.

Query Parameters Example

Figure 16: Operation Query Parameter Example

Operation: Lastline

×

AV Filter ⓘ

File Type Filter ⓘ

Run

Cancel

- **AV Filter:** Allows you to filter your results by detecting AV
- **File Type Filter:** Allows you to filter your results by detected file type

Query Results

Figure 17: Operation Query IP Address Example

Threats

Showing 1 to 10 of 12

Row count: 10 1

<input type="checkbox"/>	Name	Value
	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	Threat Name	Locky
<input type="checkbox"/>	Threat Severity	warning
<input type="checkbox"/>	Threat Class	command&control
<input type="checkbox"/>	Tag	compromised/locky
<input type="checkbox"/>	Compromised	True
<input type="checkbox"/>	Threat Name	Fareit
<input type="checkbox"/>	Tag	compromised/fareit
<input type="checkbox"/>	Threat Name	Quent Loader
<input type="checkbox"/>	Threat Class	Malware Distribution
<input type="checkbox"/>	Tag	compromised/quent loader

Previous

Next

Add Selected Attributes

Related Indicators

Showing 1 to 10 of 51

Row count: 10 1

<input type="checkbox"/>	Value	Type
	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	185.82.216.45	IP Address
<input type="checkbox"/>	31.41.44.45	IP Address
<input type="checkbox"/>	107.181.187.12	IP Address
<input type="checkbox"/>	193.9.28.13	IP Address
<input type="checkbox"/>	212.109.219.31	IP Address
<input type="checkbox"/>	5.152.199.70	IP Address
<input type="checkbox"/>	206.190.38.201	IP Address
<input type="checkbox"/>	185.117.103.176	IP Address
<input type="checkbox"/>	194.1.236.126	IP Address
<input type="checkbox"/>	216.58.216.45	IP Address

Previous

Next

Add Selected Indicators

Rate Response

Show

Figure 18: Operation Query Domain Example

Threats

Name	Value
Search	Search
Tag	popularity-rank:4
Threat Severity	info
Tag	age:19 years

Add Selected Attributes

Related Indicators

Showing 1 to 10 of 99

Row count: 10

Value	Type
Search	Search
info.com	FQDN
akmtyamfytvashaw.eu	FQDN
befhfc.eu	FQDN
bftakdpweflyhe.bid	FQDN
cpuxfemmetakvlg.eu	FQDN
csrbcmvclq.eu	FQDN
cthvmskggo.eu	FQDN
djybdapmipermtdy.bid	FQDN
dryppfdume.eu	FQDN
dqcsuwakaynnrk.eu	FQDN

Previous

Next

Add Selected Indicators

Raw Response

Show

Get Reputation

This action will allow you get a reputation query for a FQDN or IP Address.

Figure 19: Operation Query Reputation Example

Reputation Details

Name	Value
Search	Search
First Seen	2015-02-02 09:00:03
Threat Name	Zeus
Reputation Comment	Zeus (a.k.a. Zbot, PRG, Winpoem or Gorfax) is a Trojan horse malware that intercepts banking information by keystroke logging and form injection. The information is then sent to a Command and Control host. The credentials are then for example used to perform banking fraud. Zeus is spread mainly through drive-by downloads and social engineering attacks.
Last Seen	2019-03-01 21:08:56
Compromised	True
Threat Severity	100
Threat Impact	80
Threat Class	command&control

Add Selected Attributes

Raw Response

Show

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING 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 TERMS AND CONDITIONS WHEN PURCHASED. 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.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.

Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer's responsibility.

In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

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.

©2019 ThreatQuotient, Inc. All rights reserved.