

ThreatQuotient



Report Emailer Operation

Version 1.3.0

April 23, 2024

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

Warning and Disclaimer 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

Actions 10

 Send 10

 Action Parameters..... 10

 Example Email Notification 12

Change Log 13

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 © 2024 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	1.3.0
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

The Report Emler for ThreatQuotient Operation allows you to email a PDF report directly from an object in ThreatQ.

The operation provides the following action:

- **Send** - sends an email, with the PDF attachment, to the specified recipients.

The operation is compatible with the following ThreatQ objects:

- Adversaries
- Attachments
- Campaigns
- Courses of Action
- Events
- Exploit Targets
- Incidents
- Indicators
- Reports
- TTPs
- Vulnerabilities

Installation

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 whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration whl file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the 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. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Sender Email	The email you want to use to send the reports from.
Sender Password	The password associated with the sender email.
Authenticate with Username	Enable this option if you are authenticating with a username instead of email.
Sender Username	If you have enabled the Authenticate with Username option, enter the username to authenticate with. This allows you to use your username if your SMTP server expects username authentication instead of email. Leave this field blank if you are authenticating with an email.
SMTP Server	The SMTP server used by your email provider.
SMTP Port	The port associated with the SMTP server.
Default Recipients	<p>A comma-delimited list of email addresses to receive the reports.</p> <div>  <p>This parameter can be overridden when running the operation via the action dialog box.</p> </div>

Use TLS when connecting to SMTP server

Use TLS when connecting to the SMTP server. In some corporate environments, the Report Emailer operation works without authenticating with the SMTP server

Authenticate with SMTP Server

Enable this option to authenticate with the SMTP server. In some corporate environments, this operation may work without authenticating with the SMTP server.

Bypass System Proxy Settings

Enable this option to bypass system proxy settings when running this operation.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Send	Sends an email (with the PDF attachment) to the specified recipients.	Adversaries, Attachments, Campaigns, Courses of Action, Events, Exploit, Targets, Incidents, Indicators, Reports, TTPs, Vulnerabilities	N/A

Send

The action will send an email (with the PDF attachment) to the specified recipients.

Action Parameters

Set the optional parameters when running the operation:


PARAMETER	DESCRIPTION
Recipients (Override)	If needed, you can override the default recipients that were specified in the configuration page.
Email Subject (Optional)	You can override the auto-generated subject using this input.
Email Body (Optional)	You can set a body for the email here. By default, there is no body.
Send File as Attachment	File Object Types Only - Enable this option to attach the file to the email.
Context	Select the data to include in the PDF report. Options include: <ul style="list-style-type: none"> Attributes (default)


PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> • Sources (default) • Tags (default) • Descriptions (default)
Description Selection	Enter the source names for the descriptions to include in the PDF report.
Relationships	<p>Select the relationships to include in the PDF report. Options include:</p> <ul style="list-style-type: none"> • Adversaries (default) • Assets • Attack Patterns (default) • Campaigns • Course of Actions • Events • Exploit Targets • Identities • Incidents • Indicators • Intrusion Sets • Investigations • Malware (default) • Reports (default) • Signatures • Tools (default) • TTPs (default) • Vulnerabilities (default)
Max Relationships Count	The max number of relationships to include in the report.

Example Email Notification

[ThreatQ] PDF Summary Report for Adversary: Sofacy





Inbox x






tqintegrations@gmail.com

to me ▾

 8:54 AM (0 minutes ago)   

 ThreatQ Intelligence Platform
Copyright © 2018 ThreatQ, Inc. All rights reserved.


Sofacy

Overview

 Adversary

First Seen: 10/20/2017 12:45PM

Last Seen: 10/20/2017 12:45PM

 adversary-8.pdf

Change Log

- **Version 1.3.0**
 - Added the ability to include context, relationships, and description selections when generating a report.
- **Version 1.2.0**
 - Added the ability to authenticate using a username.
 - Updated the minimum ThreatQ version to 5.10.0.
- **Version 1.1.0**
 - Added the ability to send emails without authentication.
- **Version 1.0.0**
 - Initial release