

ThreatQuotient



Fidelis Elevate Operation

Version 1.2.4

September 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
- Prerequisites 7
- Installation..... 8
- Configuration 9
- Actions 10
 - Submit PCAP 11
 - Submit File 11
 - Submit Url 11
 - Close Alert 12
 - Sync Score 12
 - Add Labels..... 12
 - Get Reports..... 13
- Change Log 14

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	1.2.4
Compatible with ThreatQ Versions	>= 4.47.0
Fidelis Elevate Version	9.3.7
Support Tier	ThreatQ Supported

Introduction

The Fidelis Elevate operation manages Alerts on Fidelis and submits files and URLs for analysis. The operation can also fetch PDF and text reports for Fidelis alerts and attach them to the corresponding event in ThreatQ. The operation is designed to work in conjunction with the Fidelis Alerts CDF.

The operation provides the following actions:

- **Submit PCAP** - submits a PCAP file to Fidelis and queues it for playback.
- **Submit File** - submits a file to Fidelis and queues it for analysis.
- **Submit URL** - submits a url to Fidelis and queues it for analysis.
- **Close Alert** - closes an alert on Fidelis and adds the user who closed it as an attribute.
- **Sync Score** - sends the explicit threat score attribute value to an alert on Fidelis.
- **Add Labels** - adds the tags from a ThreatQ event to the alert on Fidelis.
- **Get Reports** - adds PDF and text reports for the Fidelis alert in a zip attachment in ThreatQ.

The operation is compatible with Files and URL type Indicators.

Prerequisites

The Fidelis Elevate operation requires the `paramiko` and `scp` modules to be installed in the Python environment.

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 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. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Host	The address of the Fidelis server.
Account Username	The username for the Fidelis account.
Account Password	The password for the Fidelis account.
SSH Username	The username for SSH access on the Fidelis server.
SSH Password	The password for SSH access on the Fidelis server.
Port	The port number to use for SSH access.
Sample Upload Directory	The directory to upload files and urls to on Fidelis.
CGI Path	The .cgi file to invoke on Fidelis. If this is left blank it will default to the <code>malware_check.cgi</code> .
Verify SSL	A boolean that turns SSL verification on/off.

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
Submit PCAP	Submits a PCAP file to Fidelis and queues it for playback.	tq_object dict: The ThreatQ object dictionary
Submit File	Submits a file to Fidelis and queues it for analysis.	tq_object dict: The ThreatQ object dictionary
Submit Url	Submits a url to Fidelis and queues it for analysis.	tq_object dict: The ThreatQ object dictionary
Close Alert	Close and alert on Fidelis and add the user who closed it as an attribute.	event dict: The ThreatQ object dictionary
Sync Score	Send the explicit threat score attribute value to an alert on Fidelis.	event dict: The event from the ThreatQ context, Explicit_Threat_Score int: The user selected explicit threat score
Add Labels	Add the tags from a ThreatQ event to the alert on Fidelis.	event dict: The ThreatQ object dictionary
Get Reports	Add PDF and text reports for the Fidelis alert in a zip attachment in ThreatQ.	event dict: The ThreatQ object dictionary

Submit PCAP

Submits a PCAP file to a Fidelis component. You can specify if you want Fidelis to playback the PCAP file upon upload. The provider will return a JSON response to verify if the request was successful.

One of the Fidelis sensors must be in PCAP mode in order to use the Submit PCAP action.

GET https://www.<Fidelis_Host>.com/j/rest/policy/pcap/components/ POST https://www.<Fidelis_Host>.com/j/rest/policy/pcap/upload/

THREATQ OBJECT TYPE

DESCRIPTION OF ACTION

Attachment: FILE

Sends a PCAP file to Fidelis for playback.

Submit File

Submits a file to Fidelis and queues it for analysis. The provider returns a JSON response verifying if the request was successful or not.

THREATQ OBJECT TYPE

DESCRIPTION OF ACTION

Attachment: FILE

Sends a file to Fidelis for sandbox analysis.

Submit Url

Submits an url to Fidelis and queues it for analysis. The provider returns a JSON response verifying if the request was successful or not.

THREATQ OBJECT TYPE

DESCRIPTION OF ACTION

Indicator: URL

Sends an URL to Fidelis for sandbox analysis.

Close Alert

Closes an alert's associated conclusion on Fidelis. The attributes 'CLOSED' and 'CLOSED_BY' are added to the event in ThreatQ, where 'CLOSED_BY' has the value of the Fidelis user who was assigned to the alert. The provider returns a JSON response verifying if the request was successful or not.

POST https://www.<Fidelis_Host>.com/j/rest/v2/alert/mgmt/

THREATQ OBJECT TYPE	DESCRIPTION OF ACTION
Event	Closes an alert on Fidelis using a Conclusion id attribute from the event.

Sync Score

Changes the Explicit Threat Score for an alert on Fidelis with the user-selected value from ThreatQ.

The user-selectable fields are:

- 1: False Positive
- 2: Not interesting
- 3: Interesting
- 4: Actionable

PUT https://<Fidelis_Host>/j/rest/v1/alert/feedback/

THREATQ OBJECT TYPE	DESCRIPTION OF ACTION
Event	Uploads the user-selected Explicit Threat Score to Fidelis.

Add Labels

Adds the tags from the ThreatQ event as labels to the alert on Fidelis. The provider returns a JSON response verifying if the request was successful or not.

PUT https://<Fidelis_Host>/j/rest/v1/alert/mgmt/

THREATQ OBJECT TYPE	DESCRIPTION OF ACTION
Event	Pulls the tags from the event and uploads them as labels to Fidelis.

Get Reports

Pulls PDF and text reports for a Fidelis alert and uploads it to the corresponding ThreatQ event as a zip attachment.

```
GET https://<Fidelis Host>/j/rest/v2/event/asset/<Alert Id>/
GET https://<Fidelis Host>/j/rest/v2/event/efsubmit/<Alert Id>/
GET https://<Fidelis Host>/j/rest/v2/event/entire_forensic/<Alert Id>/
GET https://<Fidelis Host>/j/rest/v2/event/efsubmit/<Alert Id>
GET https://<Fidelis Host>/j/rest/v2/event/sessiondata/1/<Alert Id>/
GET https://<Fidelis Host>/j/rest/v2/event/related/<Alert Id>
GET https://<Fidelis Host>/j/rest/v2/event/dpath/<Alert Id>/
POST https://<Fidelis Host>/j/rest/v2/docgen/<Alert Id>/
GET https://<Fidelis Host>/j/rest/v2/docgen/file/<Alert Id>/
```

THREATQ OBJECT TYPE

DESCRIPTION OF ACTION

Event

Pulls PDF and text reports for the Fidelis alert, compresses them into a zip archive, and attaches the zip to the event in ThreatQ.

Change Log

- **Version 1.2.4**
 - Resolved an Close Alert issue for Fidelis 9.6.x.
- **Version 1.2.3**
 - Removed the request payload for close_case to resolve authentication issues.
- **Version 1.2.2**
 - Updated integration authentication for Fidelis 9.6.x
- **Version 1.2.1**
 - Added support for multiple command posts for the **Get Reports** action.
- **Version 1.2.0**
 - Added support for multiple command posts except for the **Get Reports** action.
- **Version 1.1.2**
 - Updated endpoints for the **Get Reports**, **Add Labels**, and **Sync Score** actions.
- **Version 1.1.1**
 - Fixed a bug with PCAP playback.
 - Added new checkbox option to the Submit PCAP action that allows PCAP playback on Fidelis upon upload.
- **Version 1.1.0**
 - Added **Get Reports** action.
- **Version 1.0.0**
 - Initial release