ThreatQuotient

Fidelis Elevate Operation Guide

Version 1.0.1

April 04, 2021

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.

Contents

Versioning

- Current integration version: 1.0.1
- Supported on ThreatQ versions >= 4.47
- Fidelis Elevate version: 9.3.3

Introduction

This operation can manage alerts on Fidelis and submit materials for analysis.

Prerequisites

This 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 feed 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.
6. 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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter 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 malware_check cgi.

PARAMETER	DESCRIPTION
Verify SSL	A boolean that turns SSL verification on/off.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

ACTION	DESCRIPTION	OBJECT TYPES
submitPCAP	Submits a PCAP file to Fidelis and queues it for playback.	tq_object dict: The ThreatQ object dictionary
submitFile	Submits a file to Fidelis and queues it for analysis.	tq_object dict: The ThreatQ object dictionary
submitUrl	Submits a url to Fidelis and queues it for analysis.	tq_object dict: The ThreatQ object dictionary
closeAlert	Close and alert on Fidelis and add the user who closed it as an attribute.	event dict: The ThreatQ object dictionary
syncScore	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
addLabels	Add the tags from a ThreatQ event to the alert on Fidelis.	event dict: The ThreatQ object dictionary

submitPCAP

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

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.

submitFile

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.

submitUrl

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.

closeAlert

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 provides the following default mapping for this Action:

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

syncScore

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://www.<Fidelis_Host>.com/j/rest/v1/alert/feedback/

ThreatQ provides the following default mapping for this Action:

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

addLabels

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://www.<Fidelis_Host>.com/j/rest/v1/alert/mgmt/

ThreatQ provides the following default mapping for this Action:

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

Change Log

- **Version 1.0.1**
  - Initial Release