ThreatConnect™

FireEye® Helix™ Log Analytics Integration

Configuration Guide

Software Version 1.0

August 6, 2019

30046-03 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489

Table of Contents

OVERVIEW

The ThreatConnect® integration with FireEye Helix Log Analytics enables ThreatConnect customers to export Indicators [Address, Host, Email Address, and File (MD5 or SHA1)] to FireEye Helix Log Analytics lists for alerting and detection.

DEPENDENCIES

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) key

NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration on the** Account Settings **screen within their Private Instance of ThreatConnect.

FireEye Helix Dependencies

- Active FireEye Helix API key with the following entitlements:
  - tap.indicators.add
  - tap.indicators.delete
  - tap.indicators.edit
  - tap.indicators.browse
  - tap.indicators.read
  - tap.lists.add
  - tap.lists.browse
  - tap.lists.read

CONFIGURATION PARAMETERS

Parameter Definition

The parameters defined in Table 1 apply to the configuration parameters during the job-creation process.

Table 1

Name	Description
API User	This parameter is the name of the API user account running the app.
FireEye Helix Base Url (e.g., https://apps.fireeye.com:443)	This parameter is the Base URL to the FireEye Helix instance (e.g., https://apps.fireeye.com:443).
FireEye Helix API Token	This parameter is the FireEye Helix API token with access to the v3 API.
FireEye Helix List Name	This parameter is the FireEye Helix list name the app should modify.
FireEye Helix Customer Instance	This parameter is the FireEye Helix customer instance ID (e.g., abc123).
FireEye Helix Indicator Type	This parameter is the type of Indicator that should be added to the list. Possible choices are Address, Host, Email Address, MD5, and SHA1.
Organization(s) to be exported	This parameter is a multi-select list of ThreatConnect owners from which to pull data.
The last time this task successfully started	This parameter is the last time the job ran successfully.

Export an Indicator when its Threat Rating >= this threshold	This parameter defines a Threat Rating filter on the data being sent to FireEye Helix. Only Indicators with a Threat Rating greater than or equal to the defined value will be sent.
Export an Indicator when its Confidence Rating >= this threshold	This parameter defines a Confidence Rating filter on the data being sent to FireEye Helix. Only Indicators with a Confidence Rating greater than or equal to the defined value will be sent.
Export Indicators with Tag	This parameter defines a Tag filter on the data being sent to FireEye Helix. Only Indicators with a Tag matching the defined value will be sent.
Delete Deprecated Indicators	This parameter enables the deletion of Indicators that no longer match the filter criteria.
Logging Level	This parameter is the logging level for the app.