ThreatConnect™

Bulk Victim Create Integration

User Guide

Software Version 1.0

August 7, 2019

30036-03 EN Rev. A

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

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

©2019 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.

Table of Contents

OVERVIEW 4

DEPENDENCIES 4

ThreatConnect Dependencies 4

APPLICATION SETUP 4

Administrative Configuration 4

INSTRUCTIONS 5

CSV TEMPLATE 7

OVERVIEW

The Bulk Victim Create integration for ThreatConnect® allows users to upload a comma-separated values (CSV) file containing a list of victims and associate it with a ThreatConnect Group object such as an Incident or Threat.

DEPENDENCIES

ThreatConnect Dependencies

- Active ThreatConnect user account in an Organization
- Spaces enabled for the user's ThreatConnect instance and the user's Organization
- **TCS - Bulk Create Victim v1.1** app installed on the user's ThreatConnect instance by a System Administrator and made available to the user's Organization
- Ability to add a Spaces app
- A properly formatted CSV file that has the first row as the header row

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.

APPLICATION SETUP

Administrative Configuration

Cloud customers will need to have a System Administrator add the application as a Spaces app for them. Private Instance customers can use the instructions in the "Adding a New Space" section of Spaces to add the application as a Spaces app.

INSTRUCTIONS

1. To use the application, select the Spaces app, and then click the **Select CSV File to Upload** button (Figure 1).

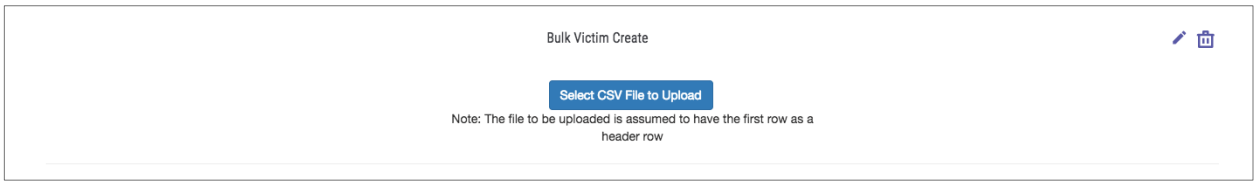

Figure 1

2. Select a CSV file for upload from the file-browsing window that appears (Figure 2).

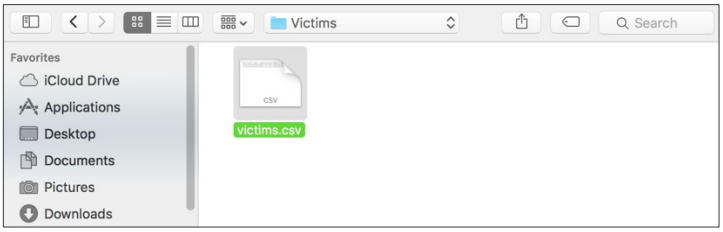

Figure 2

3. The screen will display information about the file. Use the **Choose an owner for data upload:** dropdown menu to select the owner to which to upload the data, and then click the **Import Victim Data** button (Figure 3).

Figure 3

4. Use the **Create Associations for Victim found/imported:** dropdown menu to select an existing Group object (e.g., Incident, Threat) with which to associate the imported Victims (Figure 4).

Figure 4

5. Click on the **Search** icon to display a list of recent objects of the selected type (Figure 5). Use the left and right arrows at the bottom left of the screen to navigate between pages of the list.

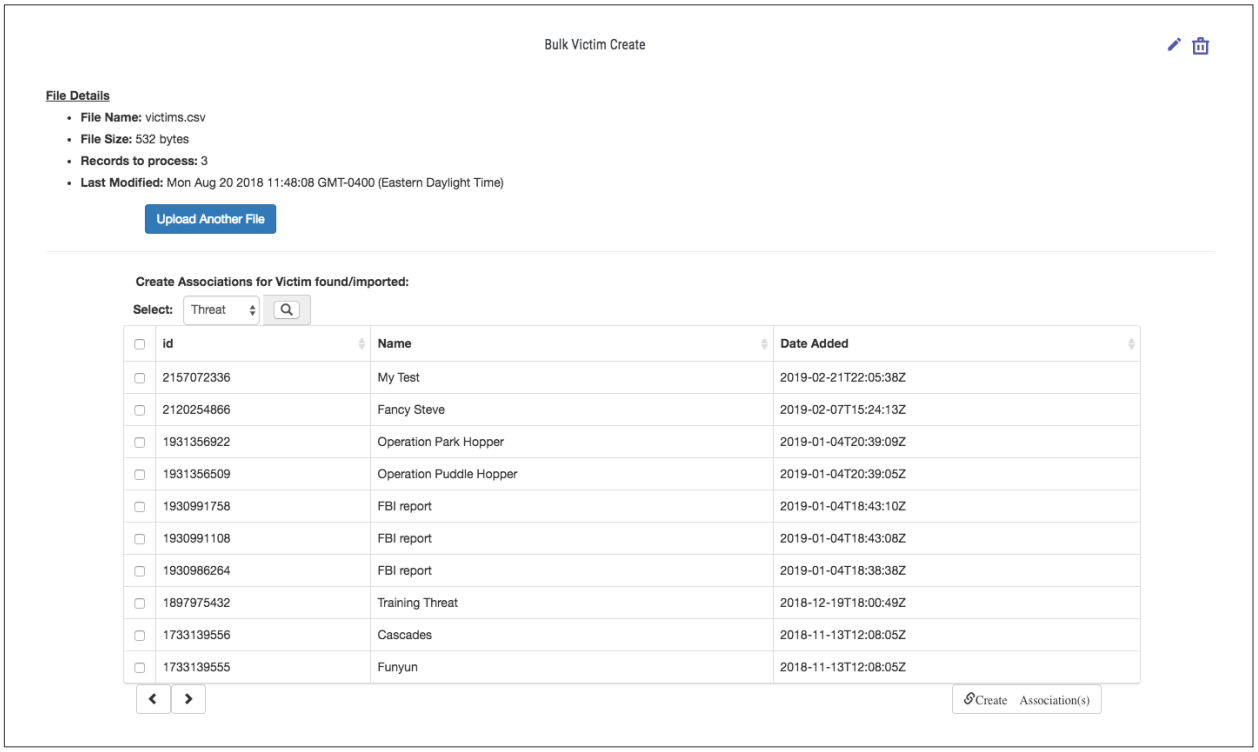

Figure 5

6. Choose one or more objects by selecting the checkbox to their left, or use the checkbox in the header row to select all objects on the page. Then click the **Create Association(s)** button at the lower right.

   NOTE: Only objects on the same page of the list may be selected together. Navigating to another list page causes selected objects from previously viewed pages to be de-selected.

7. To upload a different file, click the **Upload Another File** button.

CSV Template

The following fields may be used in the CSV file structure for Indicators:

- **Victim**: Name of Victim

  NOTE: This field is the only required field.

- **Description**: Description of Victim (e.g., "user account hacked")
- **Organization**: Organization of which Victim is a member (e.g., ABC Construction)
- **Sub-Organization**: Sub-Organization of which Victim is a member (e.g., Human Resources)
- **Nationality**: Nationality of Victim (e.g., American)
- **Work Location**: Location where Victim works (e.g., Arlington, VA)
- **E-Mail Address**: E-mail address of Victim
- **E-Mail Type**: Type of E-mail address (e.g., work, personal, etc.)
- **Social Network Account**: Social network accounts of Victim
- **Social Network Type**: Type of social network accounts (e.g., Facebook
- **Network Account**: Username of Victim (account Victim uses to log into the corresponding host system)
- **Network Type**: Type of Network (work, personal, etc.)
- **Web Site**: Victim's website
- **Phone**: Victim's phone number

In addition to the fields, the file must contain a header row that describes each column included in the file, such as in the following example:

```
Victim,Description,Organization,Nationality,Work Location,E-Mail Address,
E-Mail Type,Web Site,Phone
```

Fields that are empty for a particular victim should be marked with a single comma delimiter, with no spaces or values between. For example, the following example uses the fields chosen in the header example, but with no data for **Work Location**, **Web Site**, or **Phone**:

```
John Doe,User account hacked,Acme Corporation,American,,jdoe@acme.com,Work,,,
```

Fields that include a comma character within the field itself should be enclosed in double quotes. For example, if a **Work Location** of Arlington, VA, were added to the example, the row would look as follows:

```
John Doe,User account hacked,Acme Corporation,American,"Arlington, VA",
jdoe@acme.com,Work,,,
```