This is an updated version of Chris Frain's original script integrating HX with the iSIGHT API. Note that main arguments **must precede** the positional arguments of 'write' or 'create'. Additionally, due to a bug in Python's argparse package, the 'condition-types' argument **must not be last argument before the positional arguments**.

Version History

6.2:

1. Added an -i switch to support sourcing IOCs from the JSON formatted file in an IOC package downloaded from a report in the portal - as opposed to sourcing from the API.

6.1.1:

1. Fixed issues with unicode En Dash and Em Dash in iSIGHT report descriptions.
2. Switched the URL test condition to *contains* instead of *equal*
3. Print indicator names as they're created

main arguments:

```
  -i INPUT_FILE, --input-file INPUT_FILE
                        The path to a JSON formatted iSIGHT IOC file - as
                        opposed to sourcing from the iSIGHT API.
  --condition-types [CONDITION_TYPES [CONDITION_TYPES ...]]
                        The names of the condition type(s) to include when
                        parsing the iSIGHT report data, separated by a space.
                        Example: 'md5 domain'. Default: ['md5', 'ip', 'domain', 'url']
  -k ISIGHT_API_PUBLIC_KEY, --api-public-key ISIGHT_API_PUBLIC_KEY
                        The iSIGHT API public key. Required: True
  -n ISIGHT_API_PRIVATE_KEY, --api-private-key ISIGHT_API_PRIVATE_KEY
                        The iSIGHT API private key. Note: if you do not supply
                        one, you will be prompted for one. Required: False
  -t TIME_SPAN, --time-span TIME_SPAN
                        The time span, in days, of indicators to retreive from
                        the iSIGHT API. Required: True
  --proxy PROXY         The URI of the proxy to use in the form of
                        http://<user>:<pass>@<hostname>:<port> or
                        socks5://<user>:<pass>@<host>:<port>. Required: False
```

'create' Mode Arguments

```
-c HX_HOST, --hx-host HX_HOST
                        The IP address or fully qualified domain name of the
                        HX controller to connect to. Required: True
-p HX_PORT, --hx-port HX_PORT
                        The port on which to communicate with the HX
                        controller, defaults to: 3000. Required: False
-u HX_USERNAME, --hx-user HX_USERNAME
                        The username with which to login to the HX controller.
                        Required: True
-s HX_PASSWORD, --hx-password HX_PASSWORD
                        The password with which to login to the HX controller.
                        Note: if you do not supply one, you will be prompted
                        for one. Required: False
-m CATEGORY_NAME, --category-name CATEGORY_NAME
                        The HX indicator category name, defaults to: iSIGHT.
                        Required: False
--use-proxy-for-hx    Use the proxy specified by the proxy option for
                        communicating with the HX controller. Required: False
```

'write' mode arguments

```
  -o OUTPUT_FILE, --output-file OUTPUT_FILE
```

Output the JSON formatted response from the iSIGHT API
to a file. Required: True

For example, if you wanted to load 'ip' and 'md5' indicators from the past day to a controller named 'my-hx01.fedemo.local' with an API username of 'api_user' and a password of 'Sup3rSecret!', you would run the script as follows:

```
iSIGHT-HX_v6_2.py -k <your iSIGHT public API key here> -n
<your iSIGHT private API key here> --condition-types 'ip md5' -t 1
create -c my-hx01.fedemo.local -u api_user -s Sup3rSecret!
```