

# Threat Intelligence with MSTICPy

## Pluralsight Blue Team Tools

Author: Ian Hellen

Last revision: March 28, 2022

A Jupyter notebook and sample data is available at my GitHub repo [ianhellen/pluralsight-btt-msticpy](https://github.com/ianhellen/pluralsight-btt-msticpy)

[ianhellen/pluralsight-btt-msticpy: Pluralsight Blue Team Tools - Threat Intelligence with MSTICPy \(github.com\)](https://github.com/ianhellen/pluralsight-btt-msticpy)

## Instructions for using the Notebook

### Getting Started

In order to run the notebook you will need:

- A Python environment (Python 3.8 or later)
- Jupyter Notebook, Jupyter Lab or VSCode installed (other notebook environments should also work)
- MSTICPy version 1.7.0 or later
  - o the PowerShell code de-obfuscation functions are included in version 1.7.5 so these functions will not work with earlier versions. All other functionality is available in 1.7.0.

You can learn more about installing and configuring MSTICPy in the MSTICPy documentation:

[Getting Started — msticpy documentation](#)

### Live Queries vs. Sample Data

Sample data for all of the operations in the notebook is included in the repo – so you do not need to have a working provider to use and experiment with the notebook.

I've included representative queries that you might use on a real investigation. These are all Microsoft Sentinel queries but can be adapted for most providers. In some cases, I am using a pre-defined query (rather than in-line query text). If you want to convert the logic to suit a different provider, you can print out the query help (which includes the query text):

```
qry_prov.WindowsSecurity.query_name("?")
```

Documentation for use of different query providers is available here:

[Querying and Importing Data — msticpy documentation](#)

## Use of Threat Intelligences

One of the notebook cells in Part 1 (Account Attacks) uses a threat intelligence lookup. The example uses AlienVault OTX. For this to work, you need to have an OTX account and API key.

You need configure this value in the msticpyconfig.yaml configuration file. The instructions for configuring this are [here](#).

[Threat Intel Lookup — msticpy documentation](#)

You can, of course, skip this step without losing much.

## Sample Data and Anti-Malware

Some of the data used in the samples and in the notebook is real (but neutered) attack code. As such, if you download it to a monitored machine, it will trigger alerts from your antimalware program. In many cases the files will be quarantined.

To avoid this, add the folder where you intend to download the courseware to the excluded folders list of your antimalware program.

## Issues and problems

Please open an issue in this GitHub repo ([Issues · ianhelle/pluralsight-btt-msticpy \(github.com\)](#)) if you hit any problems.

You can also reach out to me directly [@ianhellen on Twitter](#) or email [ianhelle@microsoft.com](mailto:ianhelle@microsoft.com).