

Resources



Ian Hellen

Principal Software Development Engineer
Microsoft Threat Intelligence Center (MSTIC)

@ianhellen www.github.com/ianhelle



MSTICPy Resources

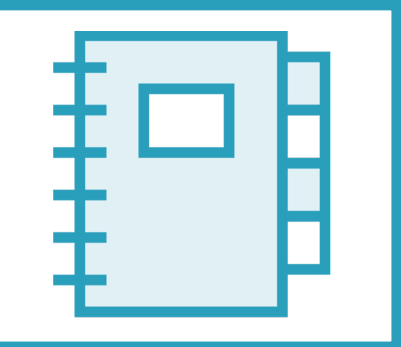


MSTICPy Documentation, <https://msticpy.readthedocs.io>



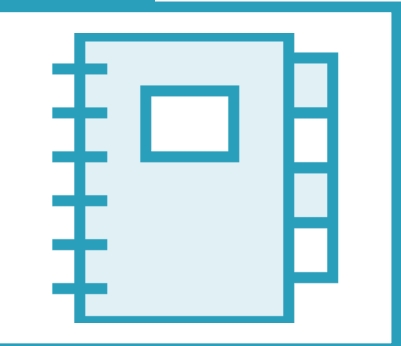
Configuring MSTICPy

https://msticpy.readthedocs.io/getting_started/SettingsEditor



Example Microsoft Sentinel Notebooks using MSTICPy

<https://github.com/azure/azure-sentinel-notebooks>



MSTICPy Feature notebooks

<https://github.com/microsoft/msticpy/tree/main/docs/notebooks>



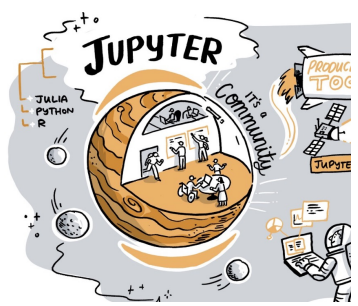
Jupyter and Python Resources



Jupyter - <https://jupyter.org>



Anaconda – <https://anaconda.com>



InfoSec Jupyterthon – Using notebooks in InfoSec Workshops

<https://infosecjupyterthon.com/>



Pandas User Guide

https://pandas.pydata.org/docs/user_guide/index.html

The Companion Notebook



GitHub Repo and Notebook

<https://bit.ly/msticpy-btt-repo>

<https://bit.ly/msticpy-btt-notebook>



MyBinder – run notebook in the cloud

<https://bit.ly/msticpy-btt-binder>



Other Resources



MITRE ATT&CK

<https://attack.mitre.org/>



Open Threat Research Forge Security Datasets

<https://securitydatasets.com>



UltimateWindowsSecurity.com

<https://www.ultimatewindowssecurity.com/securitylog/>

