FireCon 2023 Training:
Jupyter & MSTICPy in security operations and threat hunting

Your Trainers:

- **Ian Hellen**
- **Ashwin Patil**
- **(Pete Bryan – co-author but could not be with us)**

Microsoft Security Research – XSITE Team

The MSTICPy Team

Ian Hellen

Principal Software Engineer

Pete Bryan

Senior Security Researcher

Ashwin Patil

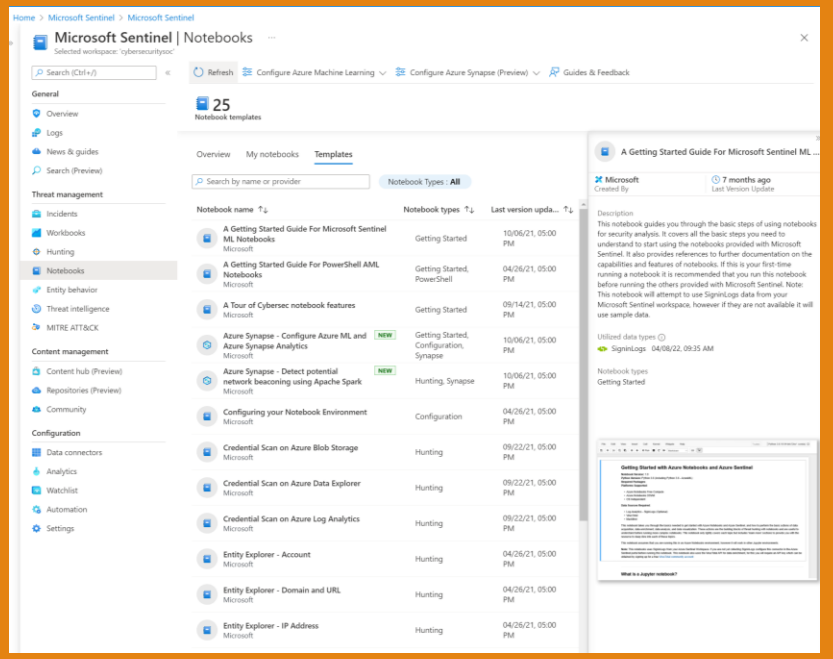
Senior Security Researcher

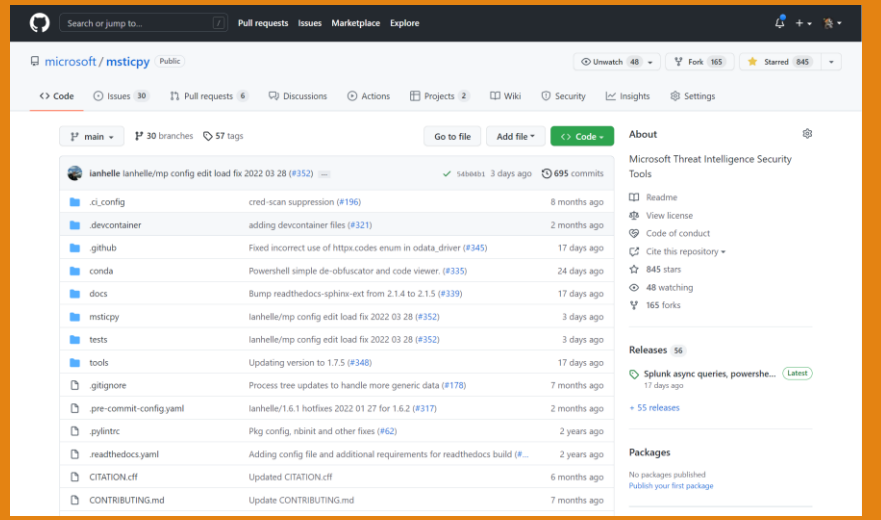
Our Community

Many & varied

History of MSTICPy

- Notebooks in Sentinel
- Need to share code with customers
- Need to maintain it
- Plenty of input and growth
  - 200k+ downloads





What's Included

Data Acquisition:

- Sentinel, Kusto, MDE, Graph
- Splunk
- More!

Data Enrichment

- Threat Intel lookups
- Context from Azure APIs
- WhoIs, GeoIP +

Analyzing Data

- Decode
- Extract
- ML: TimeSeries, Anomalies, Clustering, Beaconing

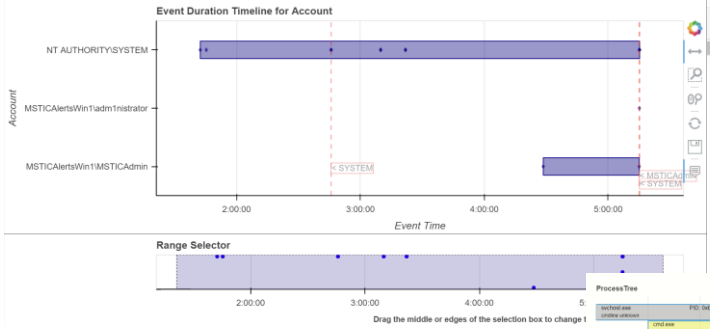
Displaying Data

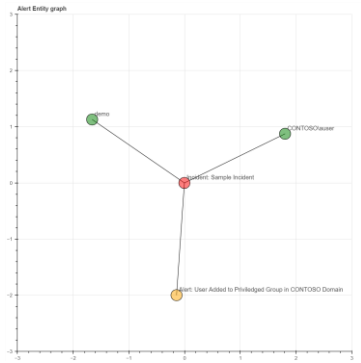
- Timelines
- Process Trees
- Graphs

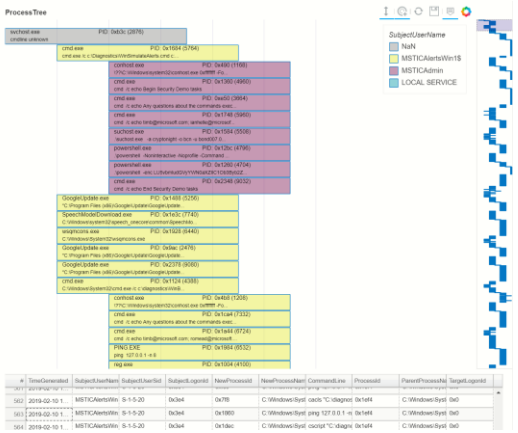
```
alerts = qry_prov.SecurityAlert.list_alerts(
    start='2019-07-21 23:43:18.274492',
    end='2019-07-27 23:43:18.274492'
)
alerts.head()
```

TimeGenerated	AlertDisplayName	Severity	Descriptio
2019-07-22 06:35:13	Suspicious authentication activity	Medium	Although r
2019-07-22 06:35:13	Suspicious authentication activity	Medium	Although r
2019-07-22 07:02:42	Traffic from unrecommended IP addresses was de...	Lo	
2019-07-26 06:03:16	Traffic from unrecommended IP addresses was de...	Lo	
2019-07-23 06:42:01	Traffic from unrecommended IP addresses was de...	Lo	

	IoC	IoCType	QuerySubtype	Result	Details
OTX	38.75.137.9	ipv4	None	True	{'pulse_count': 1, 'names': ['Ur
VirusTotal	38.75.137.9	ipv4	None	True	{'verbose_msg': 'IP address in
XForce	38.75.137.9	ipv4	None	True	{'score': 1, 'cats': {}, 'categoryD
AzSTI	38.75.137.9	ipv4	None	False	0 rows returned.
		ipv4	None	False	Not found.







The Training

The Agenda

Section	Time
Intros & Setup	15 min
Intro to MSTICPy & Notebooks	20 min
MSTICPy Configuration	15 min
Break	10 min
Acquiring data with MSTICPy	25 min
Data Visualization with MSTICPy	25 min
Enrichment with MSTICPy	20 min
Break	10 min
Data Analysis with MSTICpy	20 min
Jupyter notebooks advanced	15 min

Setup

VSCode Installed

- Juypter and Python Extensions Installed

Anaconda/Python+Jupyter Installed

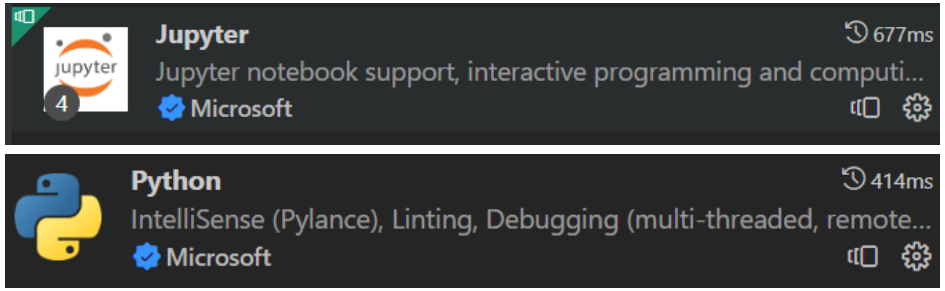
Azure CLI Installed

KeyVault Created (and details to hand)

Got API keys for:

- Alienvault OTX
- IBM Xforce
- VirusTotal
- GeoIPLite

Check you have access – https://aka.ms/sentineldemo



Setup - local Anaconda (or Python)

	Conda	Python
Open Anaconda Prompt/Terminal		
Create environment	`conda create --name msticpy python=3.11`	`python -m venv msticpy`
Activate Environment	`conda activate msticpy`	`[source] ./msticpy/scripts/activate`
Install notebooks	`conda install -c anaconda notebook`	`pip install notebook`
Clone the GitHub repo	`git clone https://github.com/microsoft/msticpy-training`	
Install packages	`pip install -r msticpy-training/requirements.txt`	
Navigate to Workshop	`cd msticpy-training/workshops/Jun2023`	
Login to Azure CLI	`az login`	
Run VSCode from here	`code .`	

Setup - Docker (VS Code or Brower)

Clone the GitHub repo

- `git clone https://github.com/microsoft/msticpy-training`

Install Docker Desktop

- https://docs.docker.com/desktop/install/windows-install/

VS Code Dev Container instructions

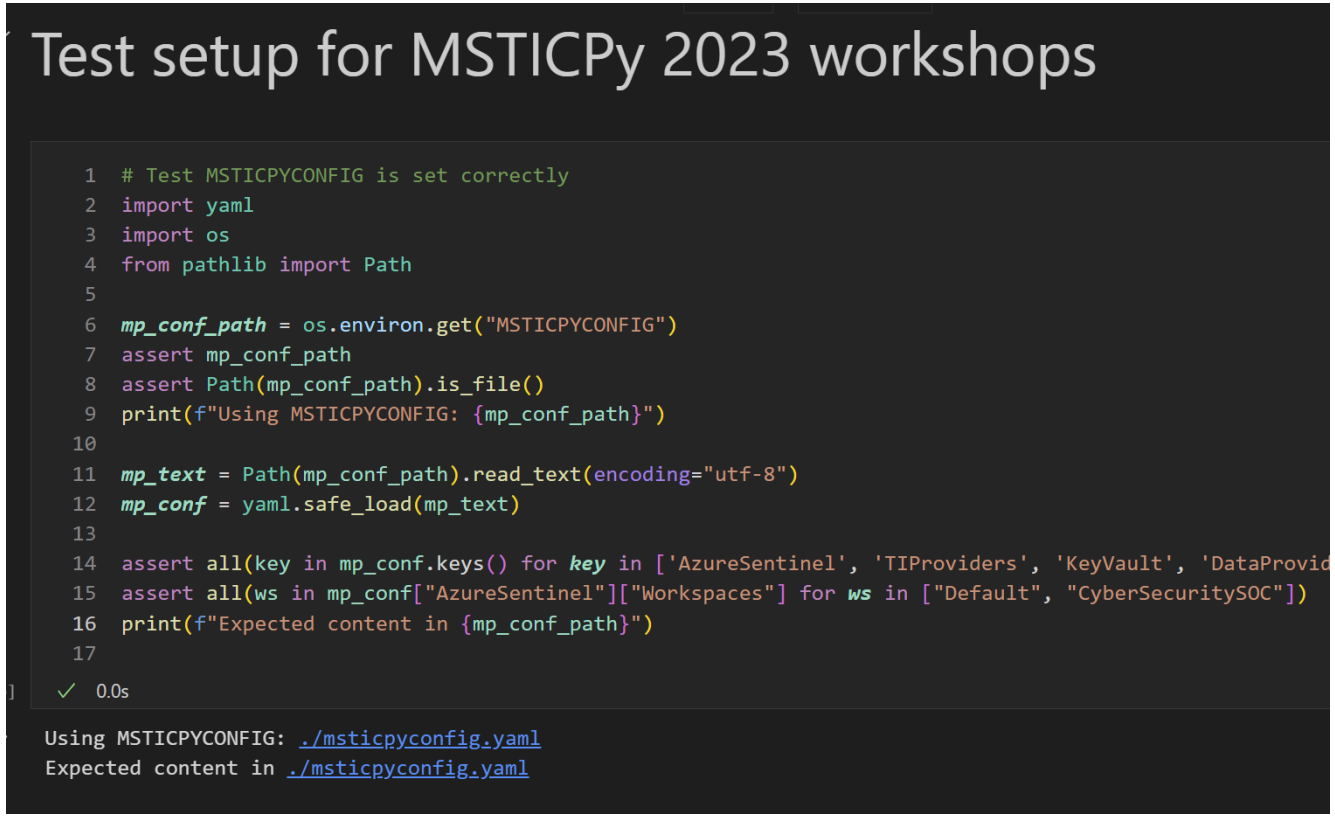
- https://github.com/microsoft/msticpy-training/blob/main/README.md

Jupyter Classic (browser) Container

- workshops/Jun2023/Docker_JupyterClassic.md

Test setup

open `workshops/Jun2023/TestSetup.ipynb` and run all cells



Questions & Issues

Use the chat for this meeting

Teams Channel - https://aka.ms/msticpy_training_teams

Breaks to Help Fix Issues

Note – if you have access to Sentinel Workspaces, Kusto Clusters, etc. feel free to use them in the course.

Start

- Go to your notebook environment
- Go to the *workshops/Jun2023* folder
- Open the *IntroToMsticpy.ipynb* file.

Summary

HOPEFULLY, YOU LEARNT SOMETHING USEFUL!

Find out more

- PyPi

https://pypi.org/project/msticpy/

- GitHub Code

https://github.com/microsoft/msticpy

- Issues

https://github.com/microsoft/msticpy/issues

- Plans

https://github.com/microsoft/msticpy/discussions

- ReadTheDocs

https://msticpy.readthedocs.io/en/latest/index.html

- msticpy@microsoft.com

Thank You