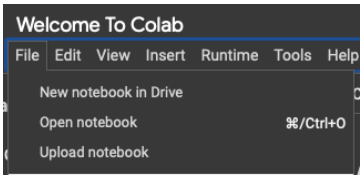
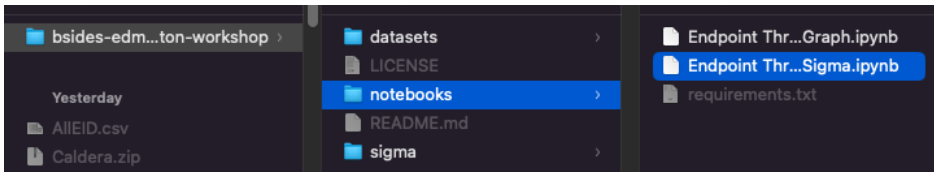
Threat Hunting with Jupyter Notebooks Workshop Demo 1

By: Kai Iyer and Meaghan Neill

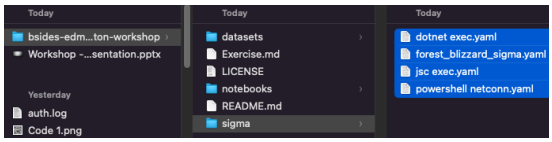
1. **Go to https://colab.research.google.com**

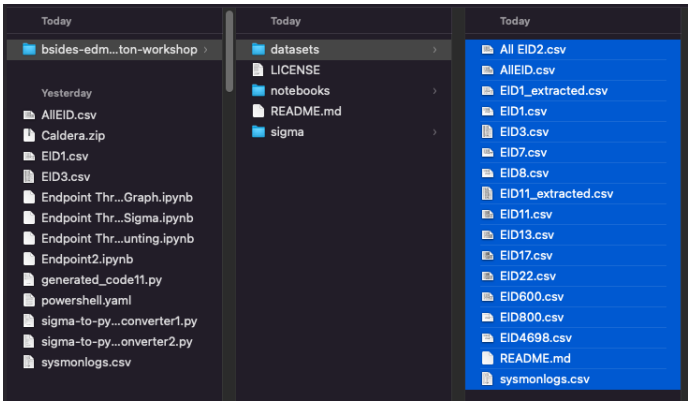
2. **Select Upload notebook, go to the folder your "bsides-edmonton-workshop" downloaded from Github, and select the "Endpoint Threat Hunting - Sigma.ipynb" notebook to open it.**





3. **Upload all the csv files from datasets and sigma for this part of the demo.**





4. **Run cell 1 to import the needed libraries.**

```
[1] import json
    import pandas as pd
    import numpy as np
```

5. **Run Cell 2 to read the csv file you are using. For our demo, we will start with EID1.csv. Later on, you will want to use different EID files to get the answers to the challenge questions.**

```
[2] df = pd.read_csv("EID1.csv")
```

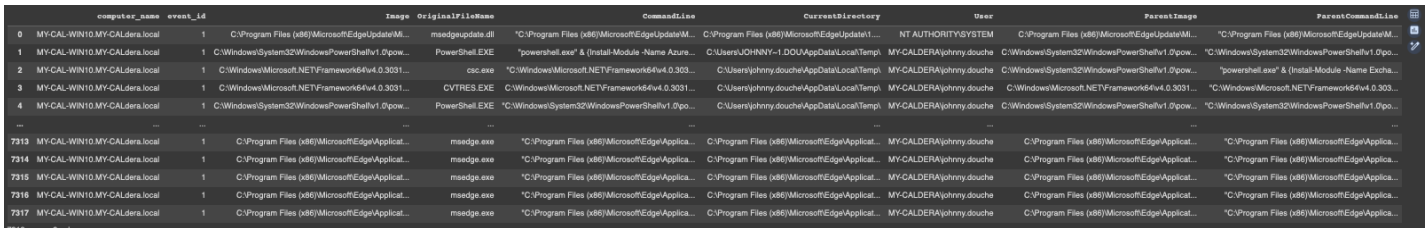
6. **Go to Cell 3. This cell extracts the EID1 Fields from Message. This can be edited for any different fields you would like to include or remove.**

```
#df = data

def extract_fields(message):
    fields = {
        'Image': None,
        'OriginalFileName': None,
        'CommandLine': None,
        'CurrentDirectory': None,
        'User': None,
        'ParentImage': None,
        'ParentCommandLine': None
    }

    if isinstance(message, str):
        for line in message.split('\n'):
            if line.startswith('Image: '):
                fields['Image'] = line.split('Image: ')[1]
            elif line.startswith('OriginalFileName: '):
                fields['OriginalFileName'] = line.split('OriginalFileName: ')[1]
            elif line.startswith('CommandLine: '):
                fields['CommandLine'] = line.split('CommandLine: ')[1]
            elif line.startswith('CurrentDirectory: '):
                fields['CurrentDirectory'] = line.split('CurrentDirectory: ')[1]
            elif line.startswith('User: '):
                fields['User'] = line.split('User: ')[1]
            elif line.startswith('ParentImage: '):
                fields['ParentImage'] = line.split('ParentImage: ')[1]
            elif line.startswith('ParentCommandLine: '):
                fields['ParentCommandLine'] = line.split('ParentCommandLine: ')[1]

    return pd.Series(fields)

extracted_df = df['message'].apply(extract_fields)

df = pd.concat([df, extracted_df], axis=1)

df.drop(columns=['message'], inplace=True)

df
```

Threat Hunting with Jupyter Notebooks Workshop Demo 1

By: Kai Iyer and Meaghan Neill

7. **Run Cell 3. This will output the EID1 Fields from Message you specified in the code.**



	computer_name	event_id	Image	OriginalFileName	CommandLine	CurrentDirectory	User	ParentImage	ParentCommandLine
0	MY-CAL-WIN10.MY-CALdera.local	1	C:\Program Files (x86)\Microsoft\EdgeUpdate\Mi...	msedgeupdate.dll	"C:\Program Files (x86)\Microsoft\EdgeUpdate\M...	C:\Program Files (x86)\Microsoft\EdgeUpdate\1....	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Microsoft\EdgeUpdate\Mi...	"C:\Program Files (x86)\Microsoft\EdgeUpdate\M...
1	MY-CAL-WIN10.MY-CALdera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"powershell.exe" & {Install-Module -Name Azure...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
2	MY-CAL-WIN10.MY-CALdera.local	1	C:\Windows\Microsoft.NET\Framework64\v4.0.3031...	csc.exe	"C:\Windows\Microsoft.NET\Framework64\v4.0.303...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"powershell.exe" & {Install-Module -Name Excha...
3	MY-CAL-WIN10.MY-CALdera.local	1	C:\Windows\Microsoft.NET\Framework64\v4.0.3031...	CVTRES.EXE	C:\Windows\Microsoft.NET\Framework64\v4.0.3031...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\Microsoft.NET\Framework64\v4.0.3031...	"C:\Windows\Microsoft.NET\Framework64\v4.0.303...
4	MY-CAL-WIN10.MY-CALdera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
...	...	...	...	...	...	...	...	...	...
7313	MY-CAL-WIN10.MY-CALdera.local	1	C:\Program Files (x86)\Microsoft\Edge\Applicat...	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Applica...	C:\Program Files (x86)\Microsoft\Edge\Applicat...	MY-CALDERA\johnny.douche	C:\Program Files (x86)\Microsoft\Edge\Applicat...	"C:\Program Files (x86)\Microsoft\Edge\Applica...
7314	MY-CAL-WIN10.MY-CALdera.local	1	C:\Program Files (x86)\Microsoft\Edge\Applicat...	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Applica...	C:\Program Files (x86)\Microsoft\Edge\Applicat...	MY-CALDERA\johnny.douche	C:\Program Files (x86)\Microsoft\Edge\Applicat...	"C:\Program Files (x86)\Microsoft\Edge\Applica...
7315	MY-CAL-WIN10.MY-CALdera.local	1	C:\Program Files (x86)\Microsoft\Edge\Applicat...	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Applica...	C:\Program Files (x86)\Microsoft\Edge\Applicat...	MY-CALDERA\johnny.douche	C:\Program Files (x86)\Microsoft\Edge\Applicat...	"C:\Program Files (x86)\Microsoft\Edge\Applica...
7316	MY-CAL-WIN10.MY-CALdera.local	1	C:\Program Files (x86)\Microsoft\Edge\Applicat...	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Applica...	C:\Program Files (x86)\Microsoft\Edge\Applicat...	MY-CALDERA\johnny.douche	C:\Program Files (x86)\Microsoft\Edge\Applicat...	"C:\Program Files (x86)\Microsoft\Edge\Applica...
7317	MY-CAL-WIN10.MY-CALdera.local	1	C:\Program Files (x86)\Microsoft\Edge\Applicat...	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Applica...	C:\Program Files (x86)\Microsoft\Edge\Applicat...	MY-CALDERA\johnny.douche	C:\Program Files (x86)\Microsoft\Edge\Applicat...	"C:\Program Files (x86)\Microsoft\Edge\Applica...

8. **Repeat Steps 5 – 7 for EID3 (Cell 4) and EID11 (Cell 5), making sure to change the file being read in Step 5.**

9. **Go to Cell 6: Credential Dumping. This is an example of what the python code will look like after using the SIGMA converter for a rule relating to Credential Dumping.**

```
[6] # Define the lists
    credential_dumping_cmd = ['crypto::certificates', 'kerberos::golden', 'kerberos::list', 'kerberos::ptt', 'lsadump::dcsync', 'lsadump::lsa', 'lsadump::sam', 'lsadump::secrets', 'mimidrv.sys', 'mimikatz', 'mimilib', 'se

    credential_dumping_cmds_combo = [
        ['procdump', '-ma'],
        ['rdrleakdiag.exe', 'fullmemdmp'],
        ['tttracer.exe', '-dumpfull']
    ]


    # Check if any of the commands in credential_dumping_cmd exist
    cmds_exist = df['CommandLine'].apply(lambda x: any(cmd in str(x) for cmd in credential_dumping_cmd) if x is not None else False)
    #print(df[cmds_exist])


    # Check if all elements of any combo exist in a row
    def check_combos(command, combo_list):

        if command is None:
            return False
        command = str(command)

        for combo in combo_list:
            if all(keyword in command for keyword in combo):
                return True
        return False

    combo_cmds_exist = df['CommandLine'].apply(lambda x: check_combos(x, credential_dumping_cmds_combo))


    ## print the alerts(if any)
    df[cmds_exist]
    #df[combo_cmds_exist]
```

10. **Run Cell 6. The output will create alerts related to Credential Dumping from the provided data.**

	computer_name	event_id	Image	OriginalFileName	CommandLine	CurrentDirectory	User	ParentImage	ParentCommandLine
56	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
90	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo %%tmp%%\...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
163	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
164	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo C:\Atomi...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
428	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo %%tmp%%\...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
446	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
821	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
866	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo %%tmp%%\...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
941	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
979	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1004	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1006	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo C:\Atomi...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1093	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo C:\Atomi...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1097	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1295	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1344	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c echo C:\Atomi...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
1460	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"cmd.exe" /c "C:\AtomicRedTeam\atomics\..\Exte...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
2034	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
2973	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
3014	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	PowerShell.EXE	"powershell.exe" & {$url='https://raw.githubus...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
3253	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"cmd.exe" /c "C:\AtomicRedTeam\atomics\..\Exte...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
4046	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"cmd.exe" /c C:\AtomicRedTeam\atomics\..\Exter...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...
4047	MY-CAL-WIN10.my-caldera.local	1	C:\AtomicRedTeam\ExternalPayloads\mimikatz\x64...	mimikatz.exe	C:\AtomicRedTeam\atomics\..\ExternalPayloads\m...	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\cmd.exe	"cmd.exe" /c C:\AtomicRedTeam\atomics\..\Exter...
4734	MY-CAL-WIN10.my-caldera.local	1	C:\Windows\System32\cmd.exe	Cmd.Exe	"C:\Windows\system32\cmd.exe" /c "C:\AtomicRed...	C:\Users\johnny.douche\AppData\Local\Temp\	MY-CALDERA\johnny.douche	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"powershell.exe" & {# starting fake DC server,...

Threat Hunting with Jupyter Notebooks Workshop Demo 1

By: Kai Iyer and Meaghan Neill

11. **Go to Cell 7: Abusing Windows Telemetry for Persistence. Windows telemetry makes use of the binary CompatTelRunner.exe to run a variety of commands and perform the actual telemetry collections. This binary was created to be easily extensible, and to that end, it relies on the registry to instruct on which commands to run. The problem is, it will run any arbitrary command without restriction of location or type. This SIGMA rule converted to Python will create alerts for any activity found within the provided data for this activity.**

```
[5]  import pandas as pd

     # Load the data
     df = pd.read_csv('EID1_extracted.csv')

     # Apply filters
     filtered_df = df[
         #(df['source_name'] == 'Microsoft-Windows-Sysmon') &
         (df['event_id'] == 1) &
         (
             df['CommandLine'].str.lower().str.contains('schtasks') |
             df['CommandLine'].str.lower().str.contains(r'\\application experience\\microsoft compatibility appraiser')
         ) &
         ~(
             df['User'].str.lower().str.contains('authori') |
             df['User'].str.lower().str.contains('autori')
         )
     ]

     result_df = filtered_df[['computer_name', 'ParentImage', 'ParentCommandLine', 'Image', 'CommandLine', 'OriginalFileName', 'CurrentDirectory', 'User']]

     result_df
```

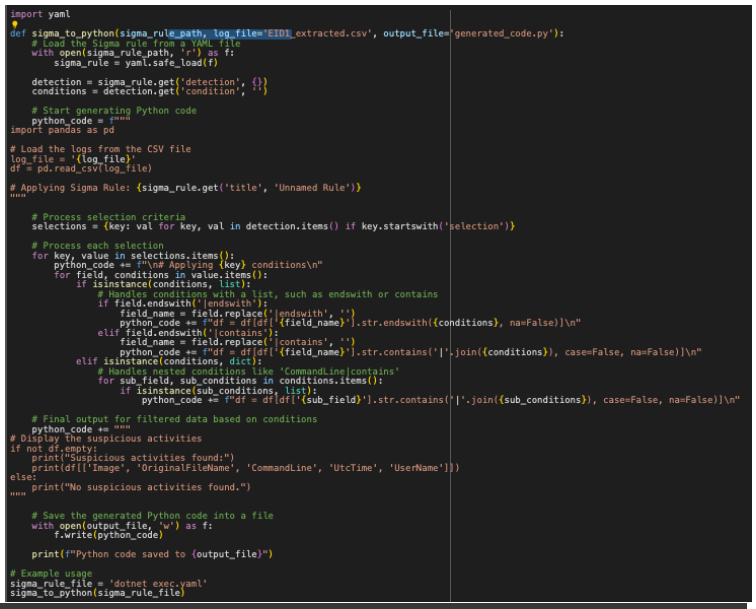
12. **Run Cell 7. The output will create alerts related to Abusing Windows Telemetry for Persistence from the provided data.**

220	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /query /xml /tn "\Micros...	C:\Windows\System32\schtasks.exe	schtasks /query /xml /tn "\Microsoft\Windows\...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
221	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /query /xml /tn "\Micros...	C:\Windows\System32\schtasks.exe	schtasks /query /xml /tn "\Microsoft\Windows\...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
225	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /query /xml /tn "\Micros...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
226	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /query /xml /tn "\Micros...	C:\Windows\System32\schtasks.exe	schtasks /query /xml /tn "\Microsoft\Windows\...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
227	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /query /xml /tn "\Micros...	C:\Windows\System32\schtasks.exe	schtasks /query /xml /tn "\Microsoft\Windows\...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
1122	MY-CAL-WIN10.my-caldera.local	C:\Program Files\Npcap\Uninstall.exe	"C:\Program Files\Npcap\uninstall.exe" /S /no_...	C:\Windows\SysWOW64\schtasks.exe	SCHTASKS.EXE /Delete /F /TN npcapwatchdog	schtasks.exe	C:\Program Files\Npcap\	MY-CALDERA\johnny.douche
1150	MY-CAL-WIN10.my-caldera.local	C:\AtomicRedTeam\ExternalPayloads\npcap_instal...	"C:\AtomicRedTeam\ExternalPayloads\npcap_insta...	C:\Windows\SysWOW64\schtasks.exe	SCHTASKS.EXE /Create /F /RU SYSTEM /SC ONSTART...	schtasks.exe	C:\Program Files\Npcap\	MY-CALDERA\johnny.douche
1442	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /create /ru system /sc d...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
1443	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /create /ru system /sc d...	C:\Windows\System32\schtasks.exe	schtasks /create /ru system /sc daily /tr "cm...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
1444	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /create /ru system /sc d...	C:\Windows\System32\schtasks.exe	schtasks /query /tn win32times	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
1455	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c reg add HKCU\SOFTWARE\ATOMIC-T105...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
1457	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c reg add HKCU\SOFTWARE\ATOMIC-T105...	C:\Windows\System32\schtasks.exe	schtasks.exe /Create /F /TN "ATOMIC-T1053.005...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
2068	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c SCHTASKS /Create /SC ONCE /TN spa...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
2069	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c SCHTASKS /Create /SC ONCE /TN spa...	C:\Windows\System32\schtasks.exe	SCHTASKS /Create /SC ONCE /TN spawn /TR C:\wi...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
2070	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c SCHTASKS /Create /S localhost /RU...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
2071	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c SCHTASKS /Create /S localhost /RU...	C:\Windows\System32\schtasks.exe	SCHTASKS /Create /S localhost /RU DOMAIN\user...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
3005	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /create /tn "T1053_005_O...	C:\Windows\System32\schtasks.exe	schtasks /create /tn "T1053_005_OnStartup" /s...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
3468	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /create /tn "T1053_005_O...	C:\Windows\System32\schtasks.exe	schtasks /create /tn "T1053_005_OnLogon" /sc ...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
3469	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks /create /tn "T1053_005_O...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
3786	MY-CAL-WIN10.my-caldera.local	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\cmd.exe /c schtasks /creat...	C:\Windows\SysWOW64\schtasks.exe	schtasks /create /tn "OpenCalcTask" /tr "C:\W...	schtasks.exe	C:\Windows\system32\	MY-CALDERA\johnny.douche
3956	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c copy %%temp%%\ExplorerSync.db %%t...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
4018	MY-CAL-WIN10.my-caldera.local	C:\Program Files (x86)\Microsoft Office\root\O...	"C:\Program Files (x86)\Microsoft Office\Root\...	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\cmd.exe /c schtasks /creat...	Cmd.Exe	C:\Windows\system32\	MY-CALDERA\johnny.douche
4278	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c copy %temp%\ExplorerSync.db %temp...	C:\Windows\System32\schtasks.exe	schtasks /create /tn ExplorerSync /tr "javaw ...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
4348	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\WindowsPowerShell\v1.0\pow...	"C:\Windows\System32\WindowsPowerShell\v1.0\po...	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks.exe /Change /TN "\Micros...	Cmd.Exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche
4349	MY-CAL-WIN10.my-caldera.local	C:\Windows\System32\cmd.exe	"cmd.exe" /c schtasks.exe /Change /TN "\Micros...	C:\Windows\System32\schtasks.exe	schtasks.exe /Change /TN "\Microsoft\Windows\...	schtasks.exe	C:\Users\JOHNNY~1.DOU\AppData\Local\Temp\	MY-CALDERA\johnny.douche

Threat Hunting with Jupyter Notebooks Workshop Demo 1

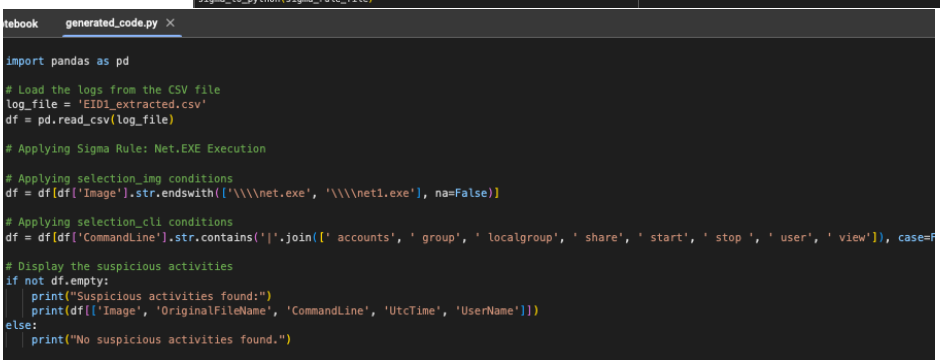
By: Kai Iyer and Meaghan Neill

13. **Go to Cell 8. This is the Sigma Converter. In this example, we are taking the "dotnet exec.yaml" file and converting it from SIGMA to python. The outputted python will be called "generated_code.py".**



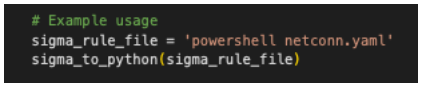
```
import yaml

def sigma_to_python(sigma_rule_path, log_file='EID1_extracted.csv', output_file='generated_code.py'):
    # Load the Sigma rule from a YAML file
    with open(sigma_rule_path, 'r') as f:
        sigma_rule = yaml.safe_load(f)

    detection = sigma_rule.get('detection', {})
    conditions = detection.get('condition', '')

    # Start generating Python code
    python_code = f"""
import pandas as pd

# Load the logs from the CSV file
log_file = '{log_file}'
df = pd.read_csv(log_file)

# Applying Sigma Rule: {sigma_rule.get('title', 'Unnamed Rule')}
"""

    # Process selection criteria
    selections = {key: val for key, val in detection.items() if key.startswith('selection')}

    # Process each selection
    for key, value in selections.items():
        python_code += f"\n# Applying {key} conditions\n"
        for field, conditions in value.items():
            if isinstance(conditions, list):
                # Handles conditions with a list, such as endswith or contains
                if field.endswith('|endswith'):
                    field_name = field.replace('|endswith', '')
                    python_code += f"df = df[df['{field_name}'].str.endswith({conditions}, na=False)]\n"
                elif field.endswith('|contains'):
                    field_name = field.replace('|contains', '')
                    python_code += f"df = df[df['{field_name}'].str.contains('|'.join({conditions}), case=False, na=False)]\n"
            elif isinstance(conditions, dict):
                # Handles nested conditions like 'CommandLine|contains'
                for sub_field, sub_conditions in conditions.items():
                    if isinstance(sub_conditions, list):
                        python_code += f"df = df[df['{sub_field}'].str.contains('|'.join({sub_conditions}), case=False, na=False)]\n"

    # Final output for filtered data based on conditions
    python_code += """
# Display the suspicious activities
if not df.empty:
    print("Suspicious activities found:")
    print(df[['Image', 'OriginalFileName', 'CommandLine', 'UtcTime', 'UserName']])
else:
    print("No suspicious activities found.")
"""

    # Save the generated Python code into a file
    with open(output_file, 'w') as f:
        f.write(python_code)

    print(f"Python code saved to {output_file}")

# Example usage
sigma_rule_file = 'dotnet_exec.yaml'
sigma_to_python(sigma_rule_file)
```

14. **Run Cell 8. It will create a generated_code.py file. As you can see, the log_file name from the function was passed here and is called EID1_extracted.csv.**

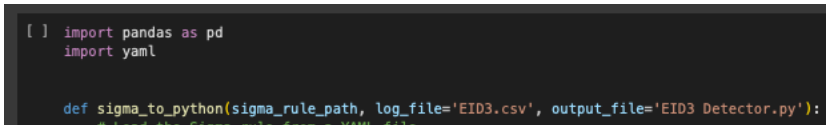


```
tebook    generated_code.py

import pandas as pd

# Load the logs from the CSV file
log_file = 'EID1_extracted.csv'
df = pd.read_csv(log_file)

# Applying Sigma Rule: Net.EXE Execution

# Applying selection_img conditions
df = df[df['Image'].str.endswith(['\\\\net.exe', '\\\\net1.exe'], na=False)]

# Applying selection_cli conditions
df = df[df['CommandLine'].str.contains('|'.join([' accounts', ' group', ' localgroup', ' share', ' start', ' stop ', ' user', ' view']), case=F

# Display the suspicious activities
if not df.empty:
    print("Suspicious activities found:")
    print(df[['Image', 'OriginalFileName', 'CommandLine', 'UtcTime', 'UserName']])
else:
    print("No suspicious activities found.")
```

15. **Repeat Steps 13 and 14 for Cell 9: EID3 to Sigma Converter. Please note that the yaml file name has been changed to "powershell netconn.yaml" and that the log_file and output_file names in the function have been changed to reflect alerts for EID3. You will want to change these fields for any of the future sigma conversions you are making.**



```
# Example usage
sigma_rule_file = 'powershell netconn.yaml'
sigma_to_python(sigma_rule_file)
```



```
[ ] import pandas as pd
    import yaml


    def sigma_to_python(sigma_rule_path, log_file='EID3.csv', output_file='EID3 Detector.py'):
```

16. **For Cell 10, these are just examples of different SIGMA schemas used for EID1. Since not all EID1 SIGMA schema is universal, it is important to take notice of what is included in the SIGMA you are working with.**