Visualizing Windows & Sysmon events

Neo4j & Python

Profile

- Transitional Period
  - Penetration Tester | Deloitte, Cyprus (Previous)
- Blog: https://medium.com/@pentesttas
- Twitter: @taso_x
- Github: https://github.com/tasox
- Creator of LogRM and Epimitheus
- Previous Talks
  - Bsides Athens, 2020
  - Bsides Cyprus, 2019
- Hobby (Jiu-Jitsu)

- “**Learning** is the path and **Knowledge** is the fuel that makes you travel a long journey of life.“

- —Sunny Jain (American player)

Introduction

Epimitheus purpose & benefits

Visualizing Windows & Sysmon events as well as enhancing the comprehension of events' generation.

Obstacles over Obstacles

Difficulties that were merged in every phase of the creation. "Too much code could break my project."

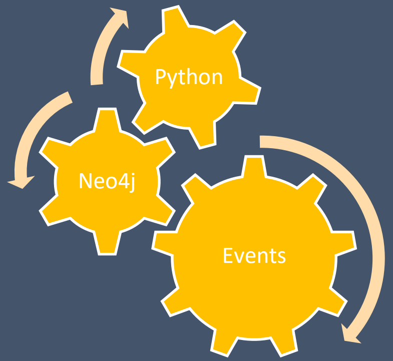
The power of Neo4j

Leverage the capabilities of Neo4j for better understanding the Windows & Sysmon events , and identify the blind spots as well.

Show, don't tell

Importing & Executing cypher queries in order to unveil famous techniques used by adversaries (MITRE ATT&CK).

Not "The Last Dance"



Epimitheus

"Is a python3 xml parser and Neo4j importer. Under the scene Epimitheus is parsing the exported .xml file of Windows and Sysmon Events, and importing all the important properties of an event into Neo4j. Plus, it connects the most important portions of an event in order to create the relationships."

MATCH p=(RemoteHosts)->(TargetUser)->(Event)->(TargetHost)

Epimitheus purpose & benefits

“What is the purpose?”

Visualizing Windows & Sysmon events that could accelerate our insight not only for Windows ecosystems but also having a superior transparency against adversaries that execute techniques based on Mitre ATT&CK.

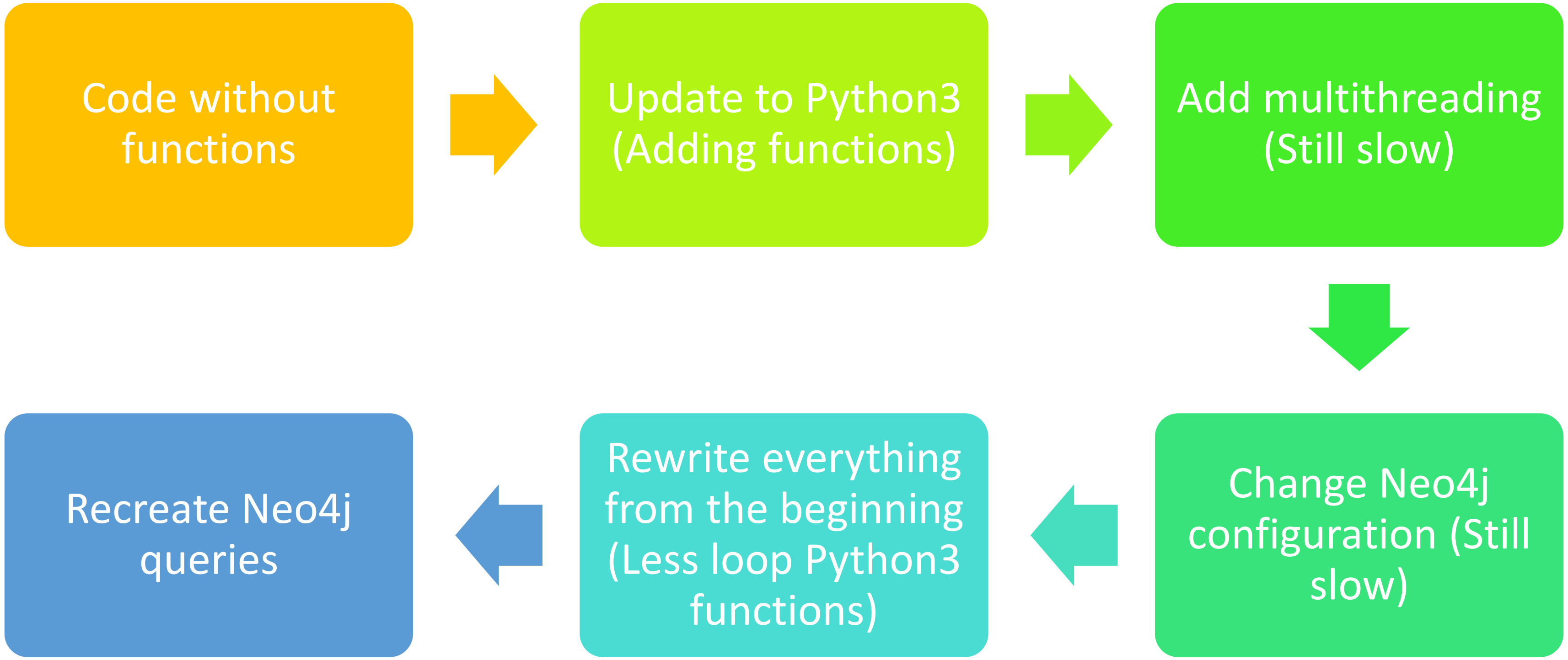
“Security Events insight”

The insight of Windows events depends on what types of events we collect, from where and how we translate them.

“What are the benefits?”

Depending on the team needs (Blue, Purple, Red) and the results that it wants to achieve.

Obstacles over Obstacles



Code without functions

Update to Python3 (Adding functions)

Add multithreading (Still slow)

Change Neo4j configuration (Still slow)

Rewrite everything from the beginning (Less loop Python3 functions)

Recreate Neo4j queries

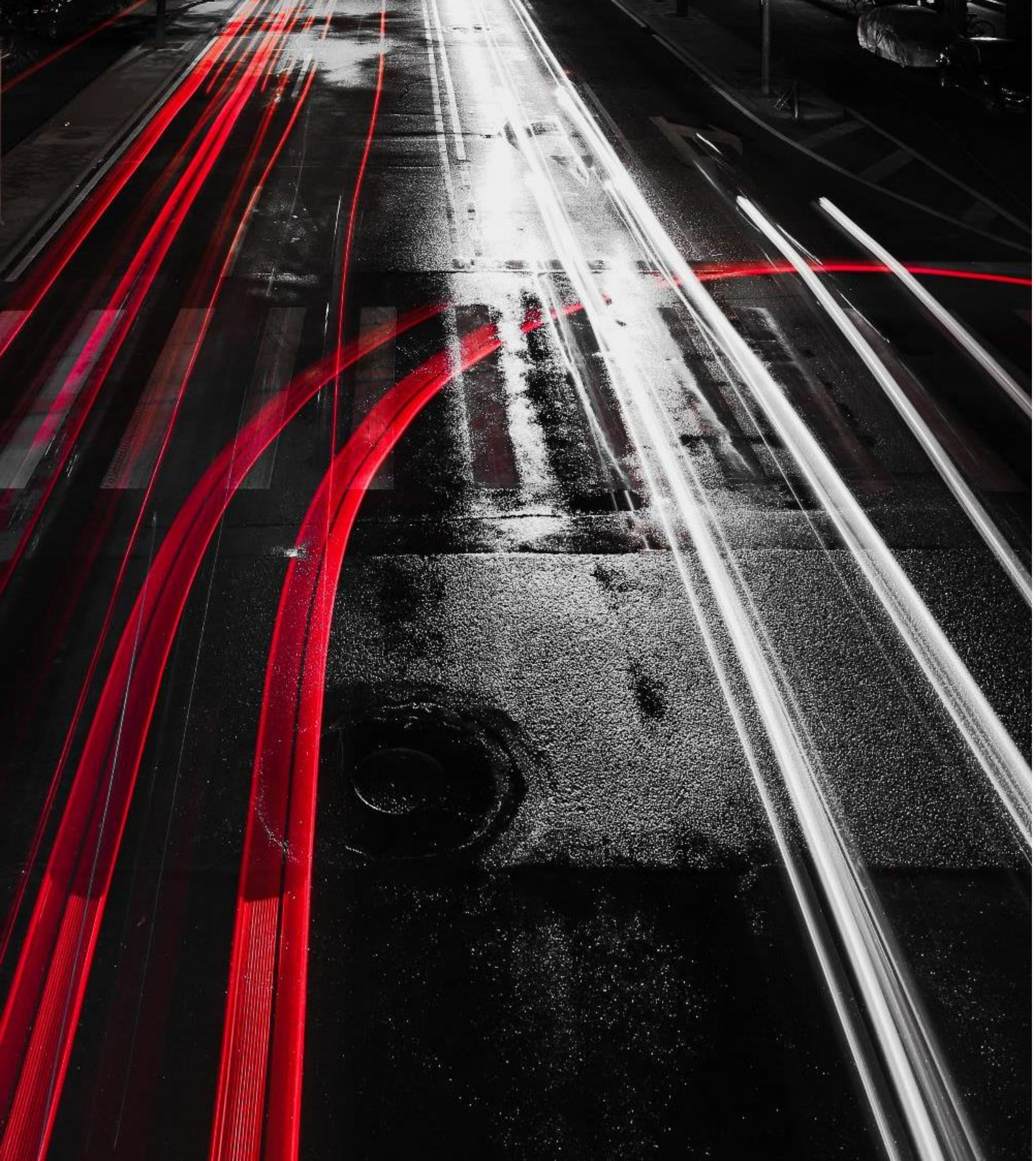
The power of Neo4j.

Easy presentation: Neo4j provides a very easy way to represent connected and semi-structured data.

Fast Execution: Connected data is very easy to retrieve and navigate.

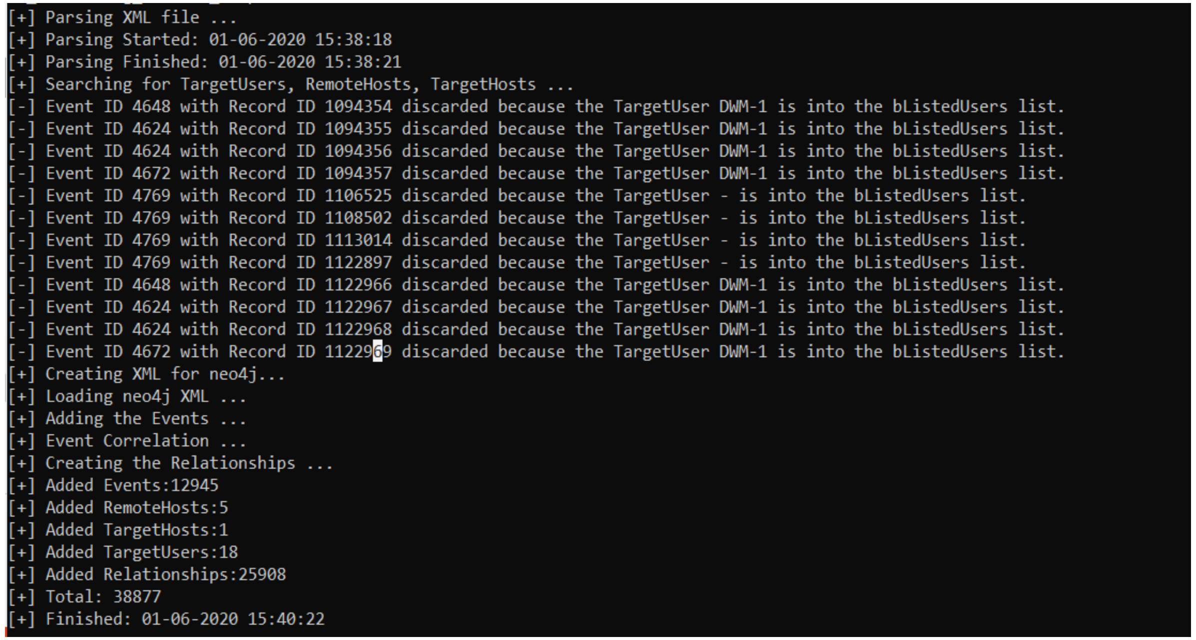
Cypher Query language: Provides CQL (Cypher Query Language) a declarative query language to represent the graph visually, using ASCII-art syntax.

No join: Doesn't require complex Joins to retrieve connected/related data.



The power of Neo4j

Performance



```
[+] Parsing XML file ...
[+] Parsing Started: 01-06-2020 15:38:18
[+] Parsing Finished: 01-06-2020 15:38:21
[+] Searching for TargetUsers, RemoteHosts, TargetHosts ...
[-] Event ID 4648 with Record ID 1094354 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4624 with Record ID 1094355 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4624 with Record ID 1094356 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4672 with Record ID 1094357 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4769 with Record ID 1106525 discarded because the TargetUser - is into the bListedUsers list.
[-] Event ID 4769 with Record ID 1108502 discarded because the TargetUser - is into the bListedUsers list.
[-] Event ID 4769 with Record ID 1113014 discarded because the TargetUser - is into the bListedUsers list.
[-] Event ID 4769 with Record ID 1122897 discarded because the TargetUser - is into the bListedUsers list.
[-] Event ID 4648 with Record ID 1122966 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4624 with Record ID 1122967 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4624 with Record ID 1122968 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[-] Event ID 4672 with Record ID 1122969 discarded because the TargetUser DWM-1 is into the bListedUsers list.
[+] Creating XML for neo4j...
[+] Loading neo4j XML ...
[+] Adding the Events ...
[+] Event Correlation ...
[+] Creating the Relationships ...
[+] Added Events:12945
[+] Added RemoteHosts:5
[+] Added TargetHosts:1
[+] Added TargetUsers:18
[+] Added Relationships:25908
[+] Total: 38877
[+] Finished: 01-06-2020 15:40:22
```

Syntax

Show, don’t tell

Import Windows Security Events:

```
Python3> Epimitheus.py –u <neo4j User> -p <neo4j Pass> -i bolt://<neo4j IP> -x <ExportedEvents.xml> -o <OutputFile.xml>
```

Import Sysmon Events (-s):

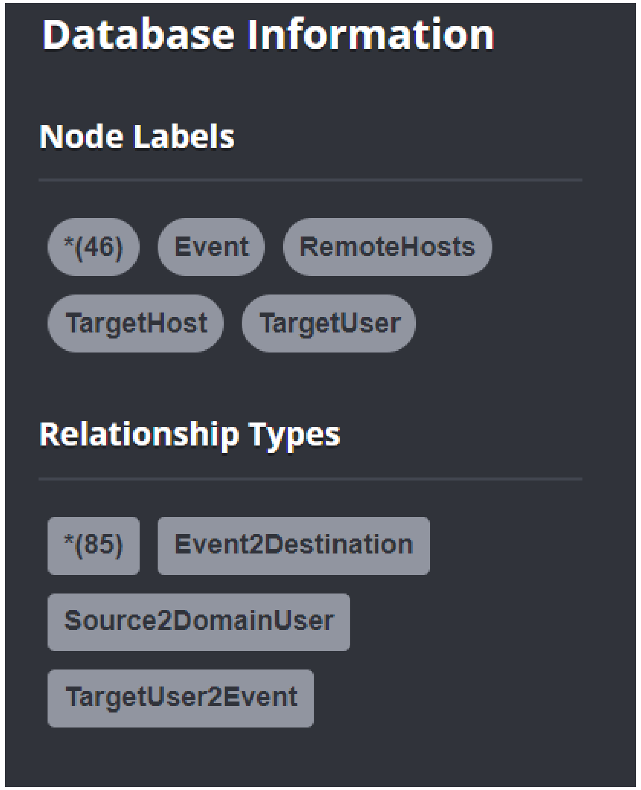
```
Python3> Epimitheus.py –u <neo4j User> -p <neo4j Pass> -i bolt://<neo4j IP> -x <ExportedEvents.xml> -o <OutputFile.xml> -s
```

Delete All from Neo4j (-D):

```
Python3> Epimitheus.py –u <neo4j User> -p <neo4j Pass> -i bolt://<neo4j IP> -D
```

Neo4j

Show, don’t tell



Database Information

Node Labels

*(46) Event RemoteHosts TargetHost TargetUser

Relationship Types

*(85) Event2Destination Source2DomainUser TargetUser2Event

Node Labels

Extracted from the events’ properties and includes 4 node labels:

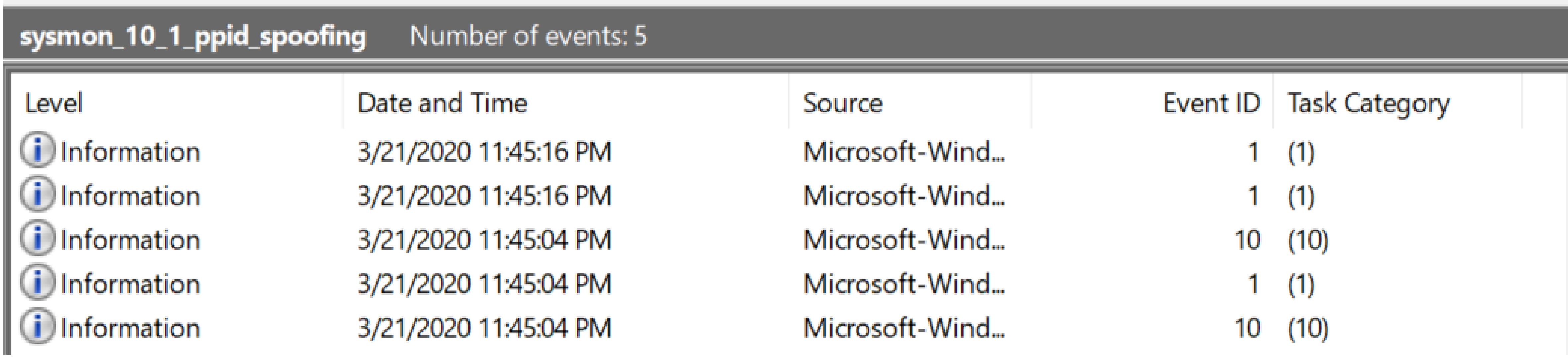
- **RemoteHosts:** From which host the event was triggered
- **TargetUser:** Which User executed the command. Every user has multiple Events
- **Event:** Containing event’s properties
- **TargetHost:** What was the destination of the triggered event.

Relationship Types

- **Source2DomainUser:** Relationship from RemoteHosts to TargetUser
- **TargetUser2Event:** Relationship from TargetUser to Event
- **Event2Destination:** Relationship from Event to TargetHost

Spot the

Show, don’t tell

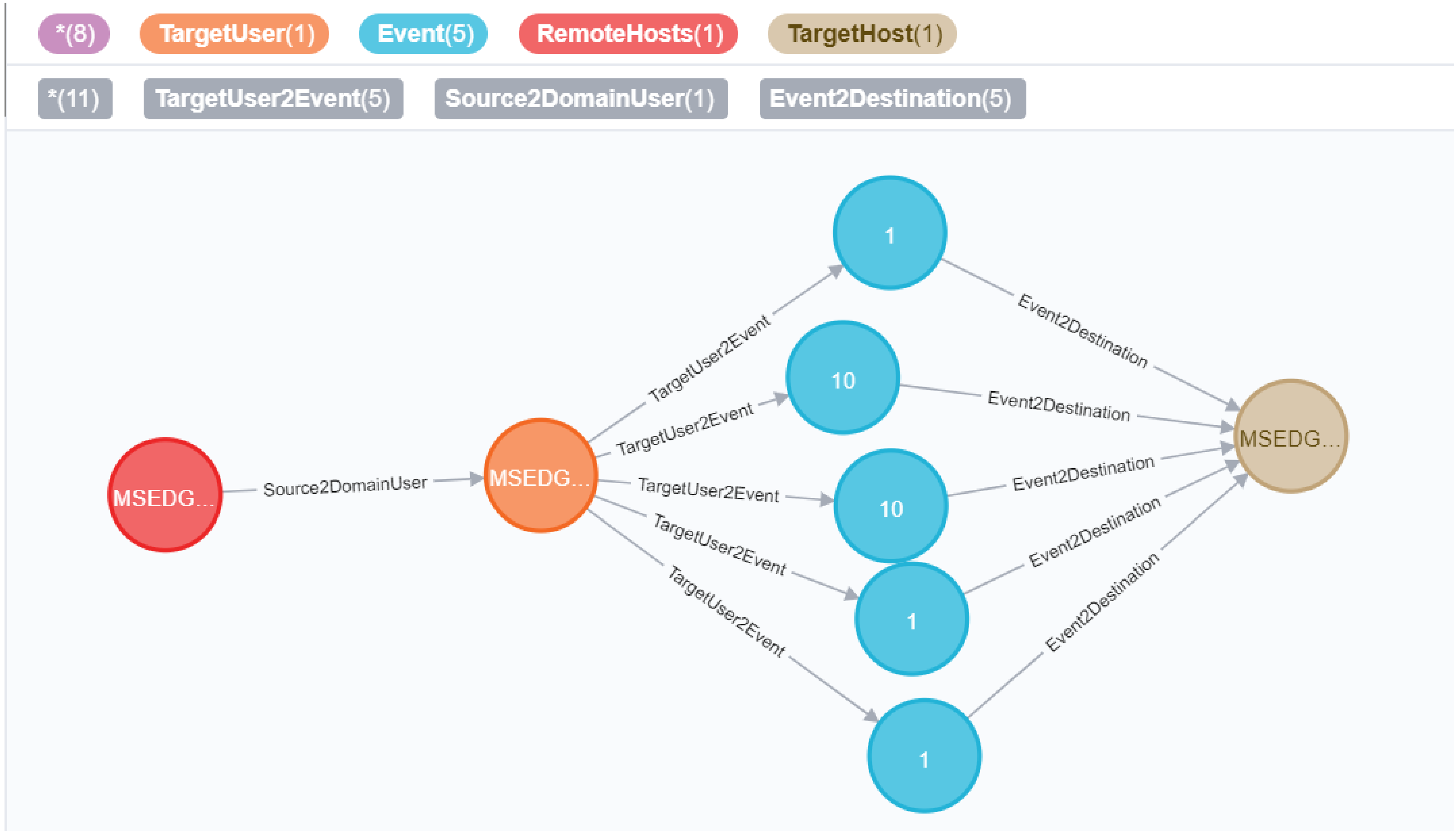


sysmon_10_1_ppid_spoofing Number of events: 5

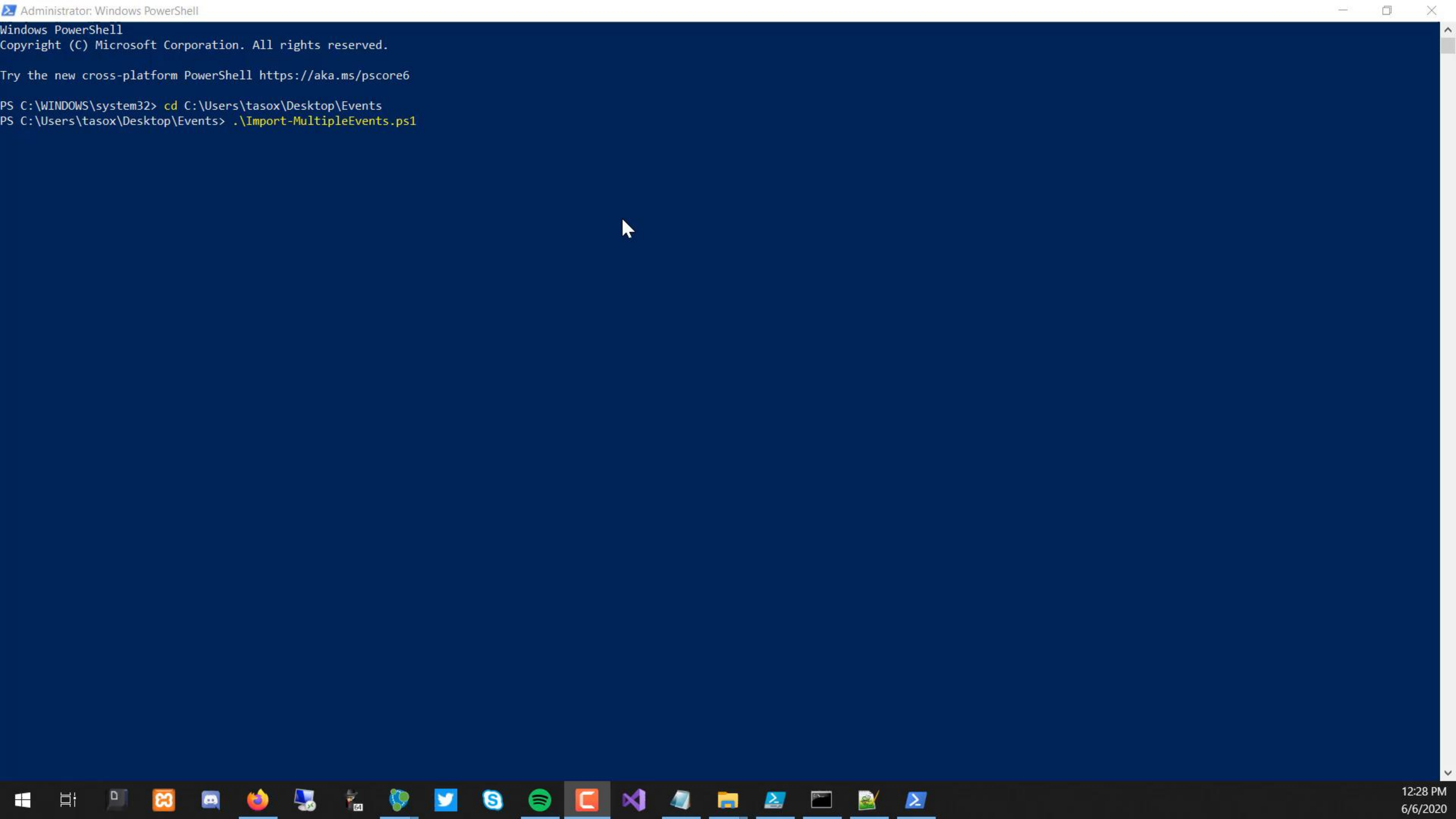
Level	Date and Time	Source	Event ID	Task Category
Information	3/21/2020 11:45:16 PM	Microsoft-Wind...	1	(1)
Information	3/21/2020 11:45:16 PM	Microsoft-Wind...	1	(1)
Information	3/21/2020 11:45:04 PM	Microsoft-Wind...	10	(10)
Information	3/21/2020 11:45:04 PM	Microsoft-Wind...	1	(1)
Information	3/21/2020 11:45:04 PM	Microsoft-Wind...	10	(10)

Difference

Show, don’t tell



IMPORT EVENTS



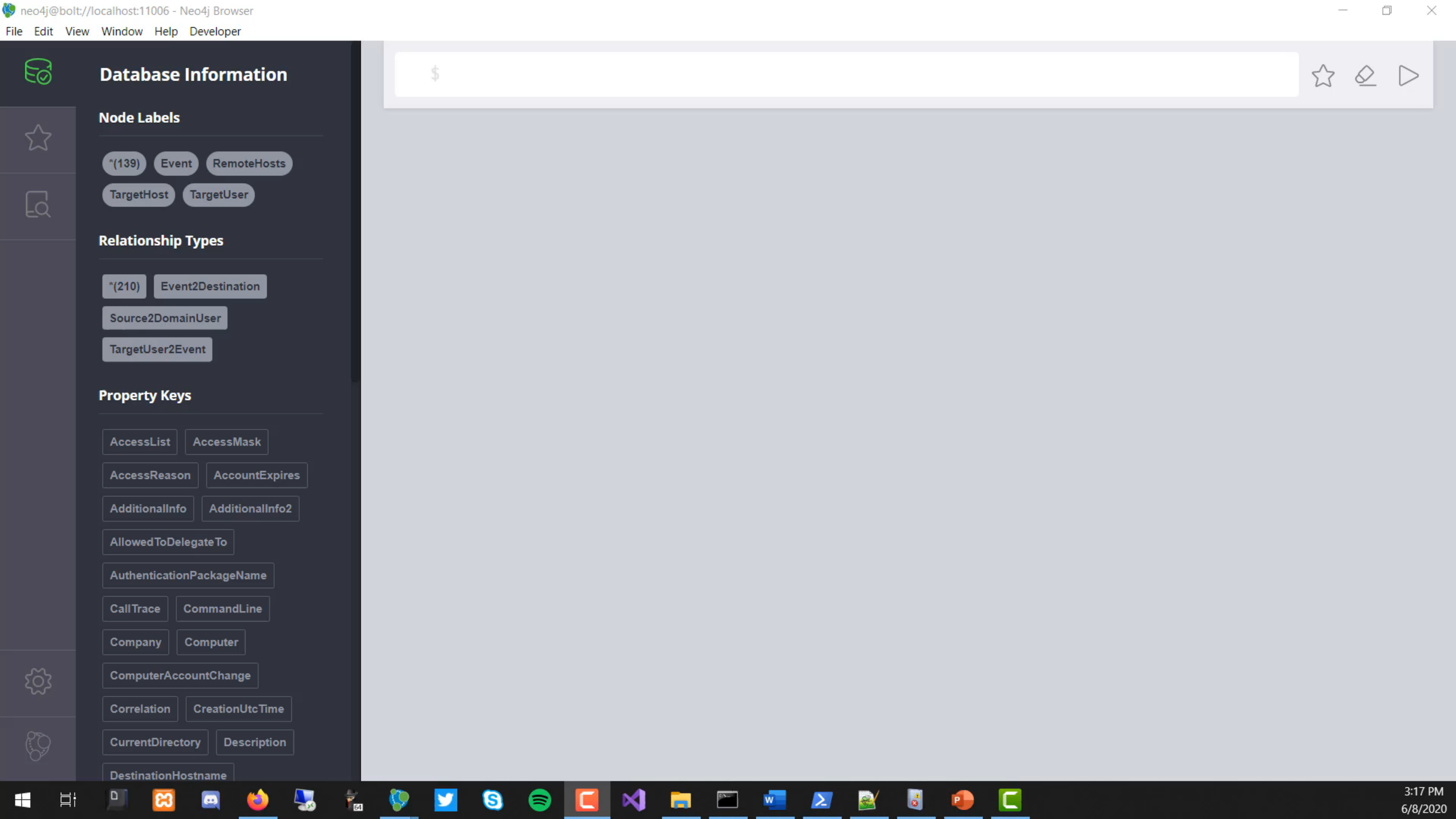
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> cd C:\Users\tasox\Desktop\Events
PS C:\Users\tasox\Desktop\Events> .\Import-MultipleEvents.ps1
```

HUNTING WITH CYPHER



Database Information

Node Labels

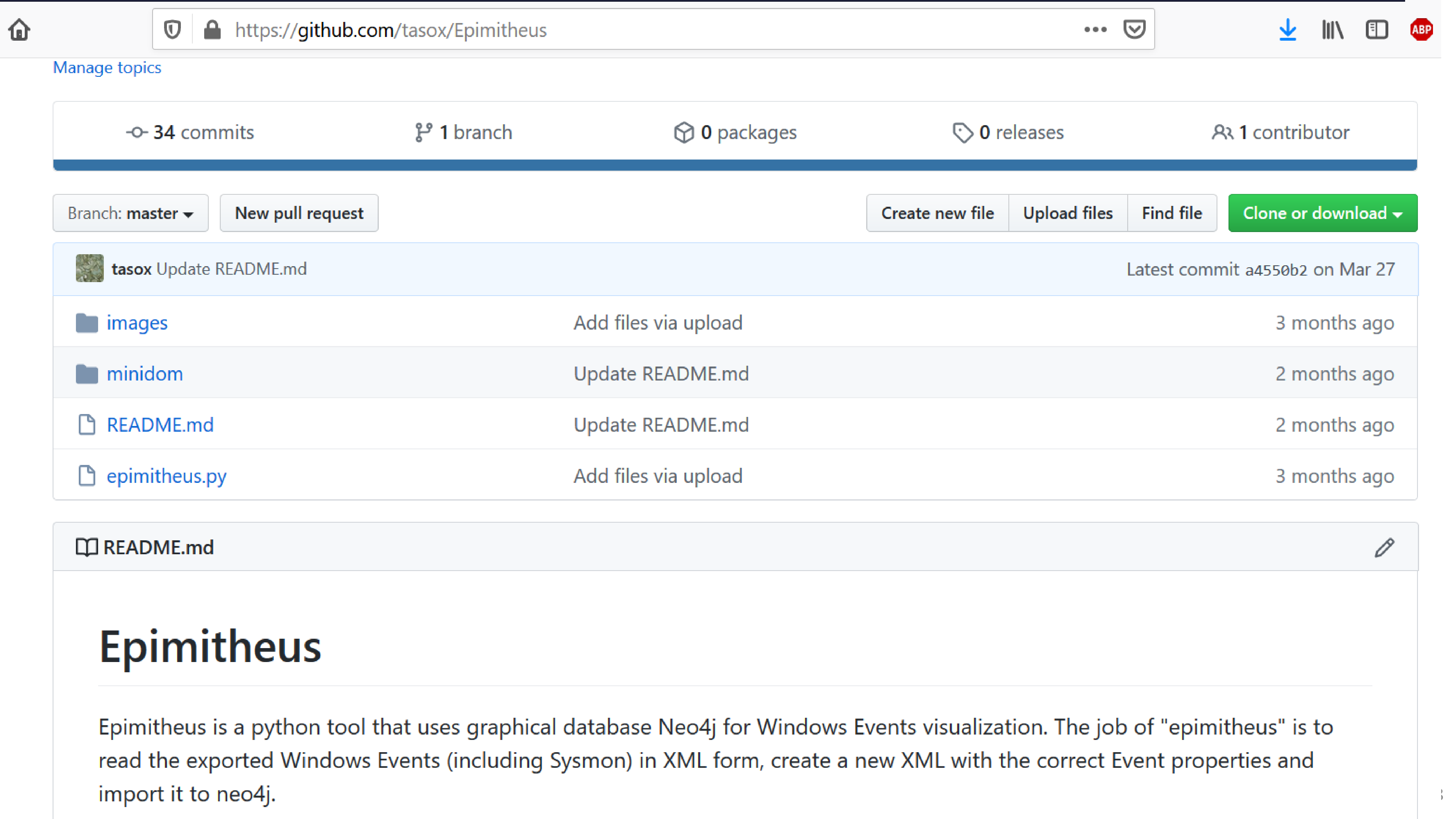
*(139) Event RemoteHosts TargetHost TargetUser

Relationship Types

*(210) Event2Destination Source2DomainUser TargetUser2Event

Property Keys

AccessList AccessMask AccessReason AccountExpires AdditionalInfo AdditionalInfo2 AllowedToDelegateTo AuthenticationPackageName CallTrace CommandLine Company Computer ComputerAccountChange Correlation CreationUtcTime CurrentDirectory Description DestinationHostname



tasox Update README.md Latest commit a4550b2 on Mar 27

images	Add files via upload	3 months ago
minidom	Update README.md	2 months ago
README.md	Update README.md	2 months ago
epimitheus.py	Add files via upload	3 months ago

README.md

Epimitheus

Epimitheus is a python tool that uses graphical database Neo4j for Windows Events visualization. The job of "epimitheus" is to read the exported Windows Events (including Sysmon) in XML form, create a new XML with the correct Event properties and import it to neo4j.

Not “The Last Dance”

Upcoming Extensions

- Dynamically export/import (Agent)
- User-friendly dashboard
- More queries based on Mitre ATT&CK
- Construct attack paths through Events

Resources:

Epimitheus

- https://github.com/tasox/Epimitheus

Posts

- https://medium.com/@pentesttas/windows-events-sysmon-visualization-using-neo4j-part-1-529ca5ab4593
- https://medium.com/@pentesttas/windows-events-sysmon-visualization-using-neo4j-part-2-d4c2fd3c9413

Event Samples & Samples of tests based on Mitre ATT&CK

- https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES
- https://github.com/redcanaryco/atomic-red-team

Thank you!

BSIDES

KØBENHAVN