Ready to ATT&CK?

Bring Your Own Data (BYOD) and Validate Your Data Analytics!

@Cyb3rWard0g & @Cyb3rPandaH

- Projects
  - @HunterPlaybook
  - @THE_HELK
  - ATTACK-Python-Client
  - @OSSEM_Project
  - @Mordor_Project
  - OpenHunt
  - Blacksmith & More
- Founders:
  - @HuntersForge

Agenda

- Explore ATT&CK
  - 2018 -> 2019
- ATT&CK Data Sources Opportunities
- Enter Mordor
- Mordor & CAR
- CAR & Threat Hunter Playbook (Notebooks)
- Hunters Forge!

Explore ATT&CK

How do I query ATT&CK?

Exploring ATT&CK Metadata!

How do I access ATT&CK Metadata?

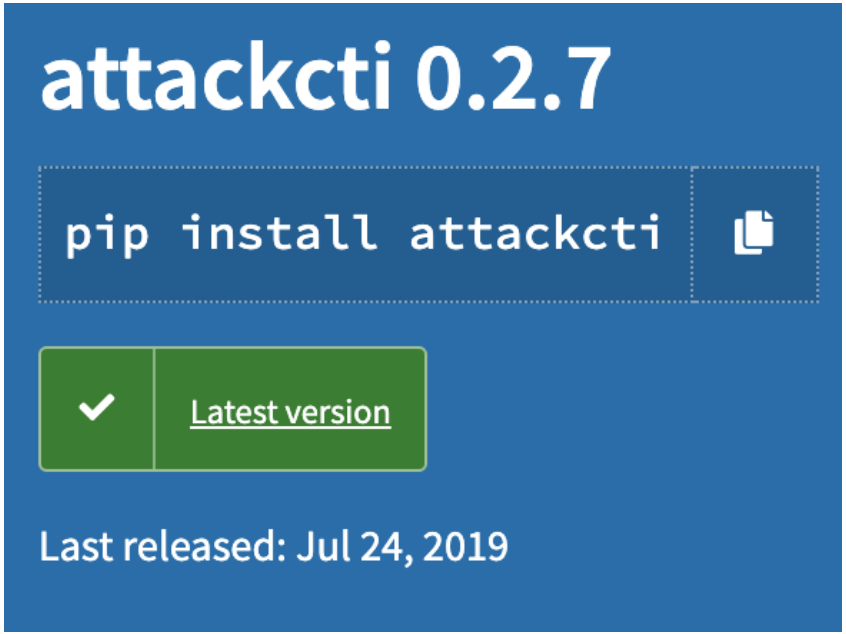
ATTACK-Python-Client Github Project

- A Python module to access up to date ATT&CK content available in STIX via public TAXII server. It leverages **cti-python-stix2** and **cti-taxii-client python** libraries developed by MITRE.
- **Goals**
  - Allow the integration of ATT&CK content with other platforms
  - Allow security analysts to quickly explore ATT&CK content and apply it in their daily operations
  - Explore all available ATT&CK metadata at once
  - Learn STIX2 and TAXII Client Python libraries

https://github.com/hunters-forge/ATTACK-Python-Client

ATTACK-Python-Client Installation

- **Via PIP:** *pip install attackcti*
- **Or Straight from Source**
  - *git clone https://github.com/hunters-forge/ATTACK-Python-Client*
  - *cd ATTACK-Python-Client*
  - *pip install .*
- **Jupyter Notebooks Available**
  - *pip install -r requirements.txt*
  - *cd notebooks*
  - *jupyter lab*

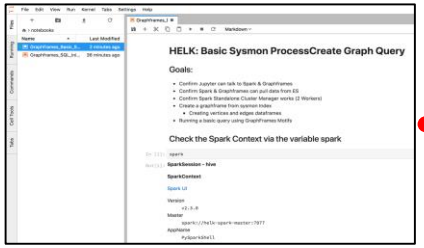


Some Available Functions

- get_enterprise
- get_enterprise_techniques
- get_enterprise_mitigations
- get_enterprise_groups
- get_enterprise_malware
- get_enterprise_tools
- get_enterprise_relationships
- get_enterprise_tactics
- get_pre
- get_pre_techniques
- get_pre_groups
- get_pre_relationships
- get_pre_tactics
- get_mobile
- get_mobile_techniques
- get_mobile_mitigations
- get_mobile_groups
- get_mobile_malware
- get_mobile_tools
- get_mobile_relationships
- get_mobile_tactics
- get_data_sources
- get_techniques_by_datasources

https://attackcti.readthedocs.io/en/latest/attackcti_functions.html

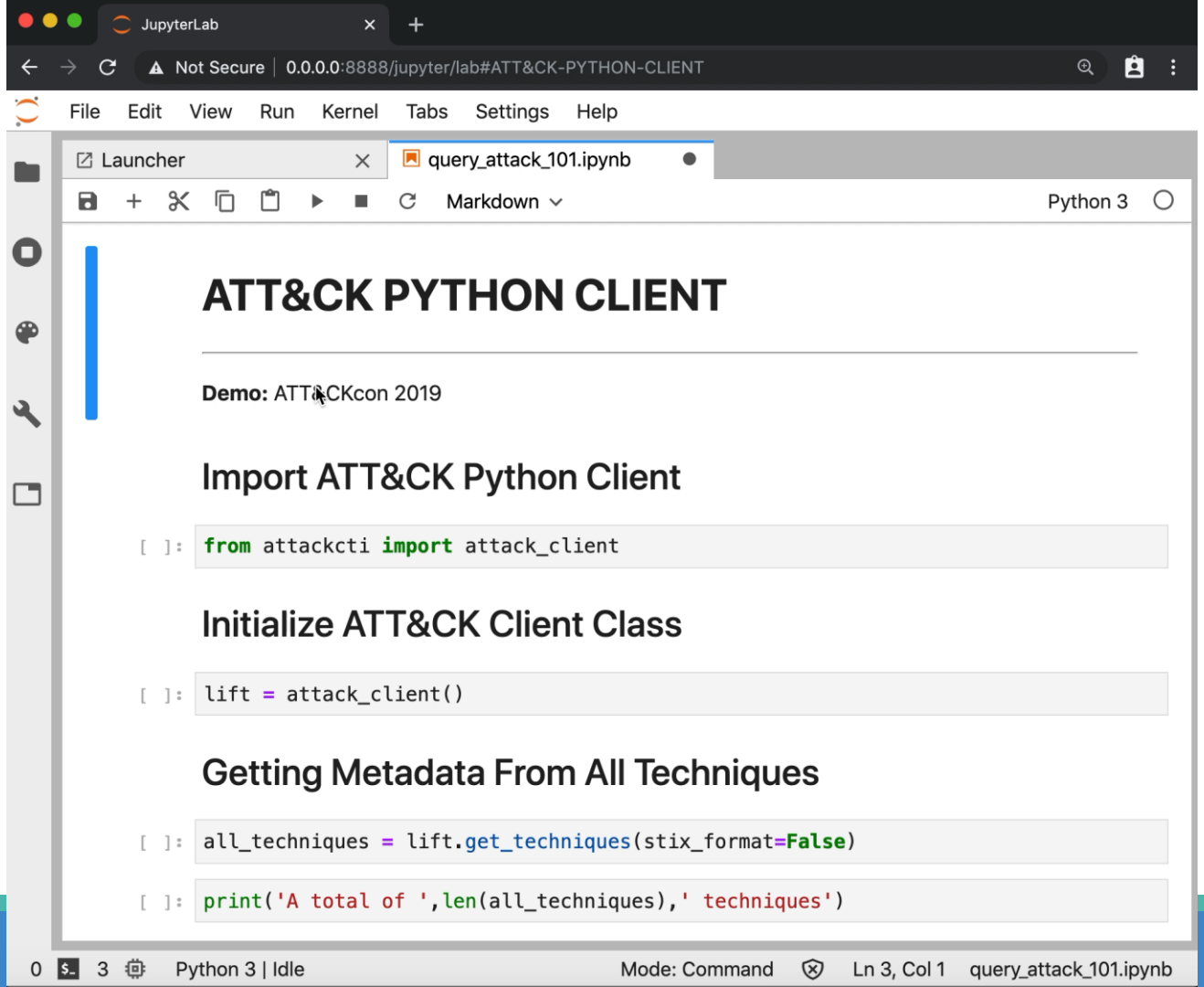
ATT&CK Metadata - Jupyter Notebook



https://github.com/hunters-forge/ATTACK-Python-Client/tree/master/notebooks

Explore ATT&CK

Querying ATT&CK 101


JupyterLab
Not Secure 0.0.0.0:8888/jupyter/lab#ATT&CK-PYTHON-CLIENT
File Edit View Run Kernel Tabs Settings Help
Launcher
query_attack_101.ipynb
Markdown
Python 3
ATT&CK PYTHON CLIENT
Demo: ATT&CKcon 2019
Import ATT&CK Python Client
[ ]: from attackcti import attack_client
Initialize ATT&CK Client Class
[ ]: lift = attack_client()
Getting Metadata From All Techniques
[ ]: all_techniques = lift.get_techniques(stix_format=False)
[ ]: print('A total of ',len(all_techniques),' techniques')
0 3 Python 3 | Idle Mode: Command Ln 3, Col 1 query_attack_101.ipynb

File Edit View Run Kernel Tabs Settings Help

query_attack_database.ipy | Untitled.ipynb | Untitled1.ipynb

Code | Python 3

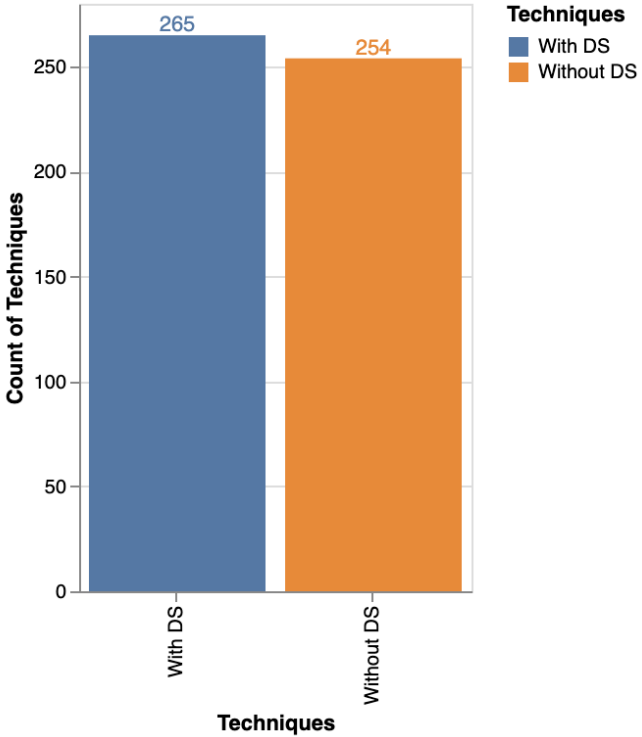
```
[ ]: from attackcti import attack_client
     from googletrans import Translator

[ ]: lift = attack_client()

[ ]: all_techniques = lift.get_techniques(stix_format=False)
     all_techniques = lift.remove_revoked(all_techniques)

[ ]: needs_translation = []
     translated = []
     for t in all_techniques:
         try:
             translator = Translator()
             espanol = translator.translate(t['technique'], dest='es')
             translated.append(espanol.text)
             print("From: ", t['technique']," To: ",espanol.text)
         except:
             needs_translation.append(t['technique'])
             continue

[ ]:
```

0 $_ 3 Python 3 | Idle Mode: Command Ln 1, Col 1 Untitled1.ipynb

Explore ATT&CK

Any New Data Sources?

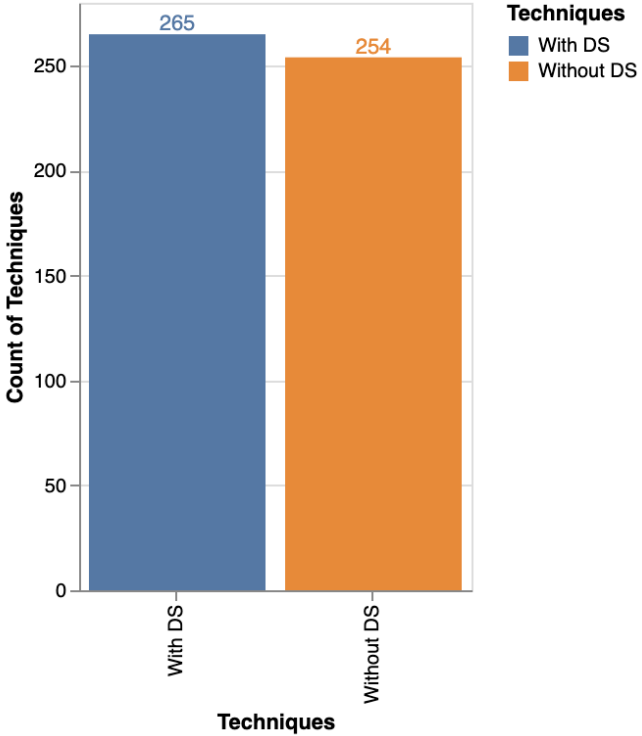
ATT&CK Techniques (519) and Data Sources

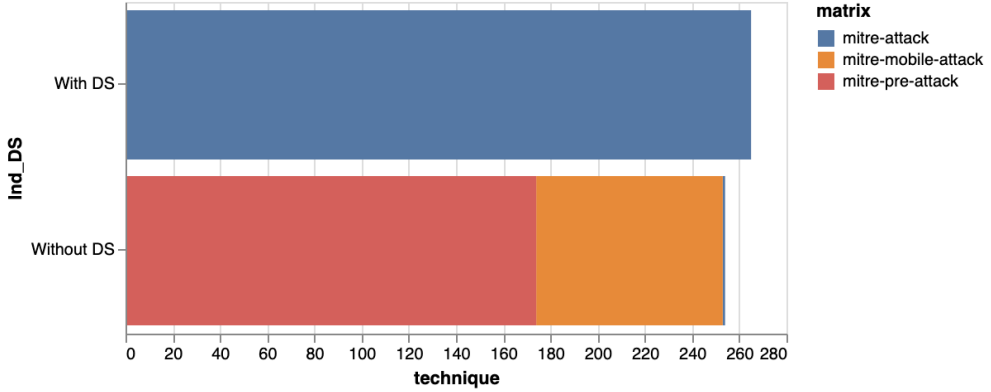


- Almost **51%** of techniques have data sources defined
- Around **49%** of techniques do **NOT** have data sources defined
- Pre-ATT&CK data sources maybe?
- Opportunities to collaborate and define those without data sources?

https://github.com/hunters-forge/ATTACK-Python-Client/blob/master/notebooks/ATT%26CK_DataSources.ipynb

ATT&CK Techniques (519) and Data Sources





	matrix	Ind_DS	technique
0	mitre-attack	With DS	265
1	mitre-attack	Without DS	1
2	mitre-mobile-attack	Without DS	79
3	mitre-pre-attack	Without DS	174

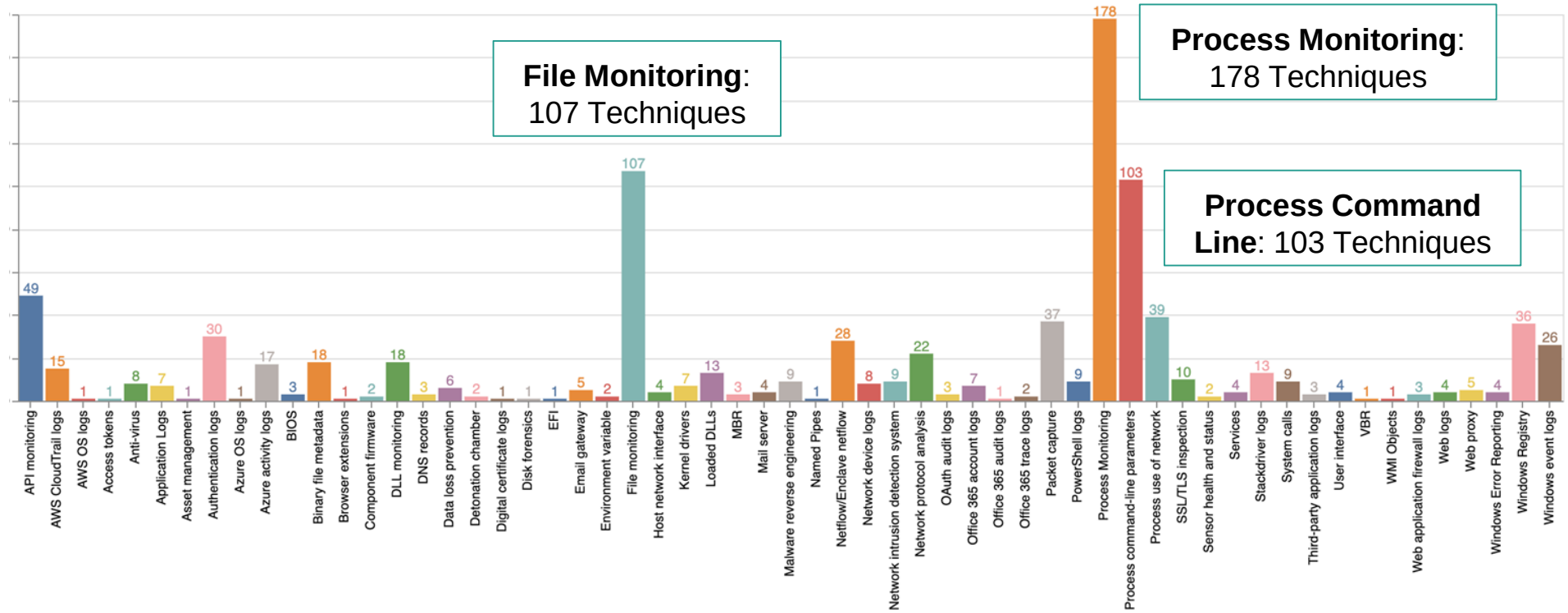
https://github.com/hunters-forge/ATTACK-Python-Client/blob/master/notebooks/ATT%26CK_DataSources.ipynb

Looking for anything to do this weekend?

	matrix	platform	tactic	technique	technique_id	data_sources	Count_DS	Ind_DS
11	mitre-attack	[GCP, Azure, AWS]	[persistence]	Implant Container Image	T1525	NaN	NaN	Without DS

https://github.com/hunters-forge/ATTACK-Python-Client/blob/master/notebooks/ATT%26CK_DataSources.ipynb

ATT&CK Techniques with Data Sources (265)

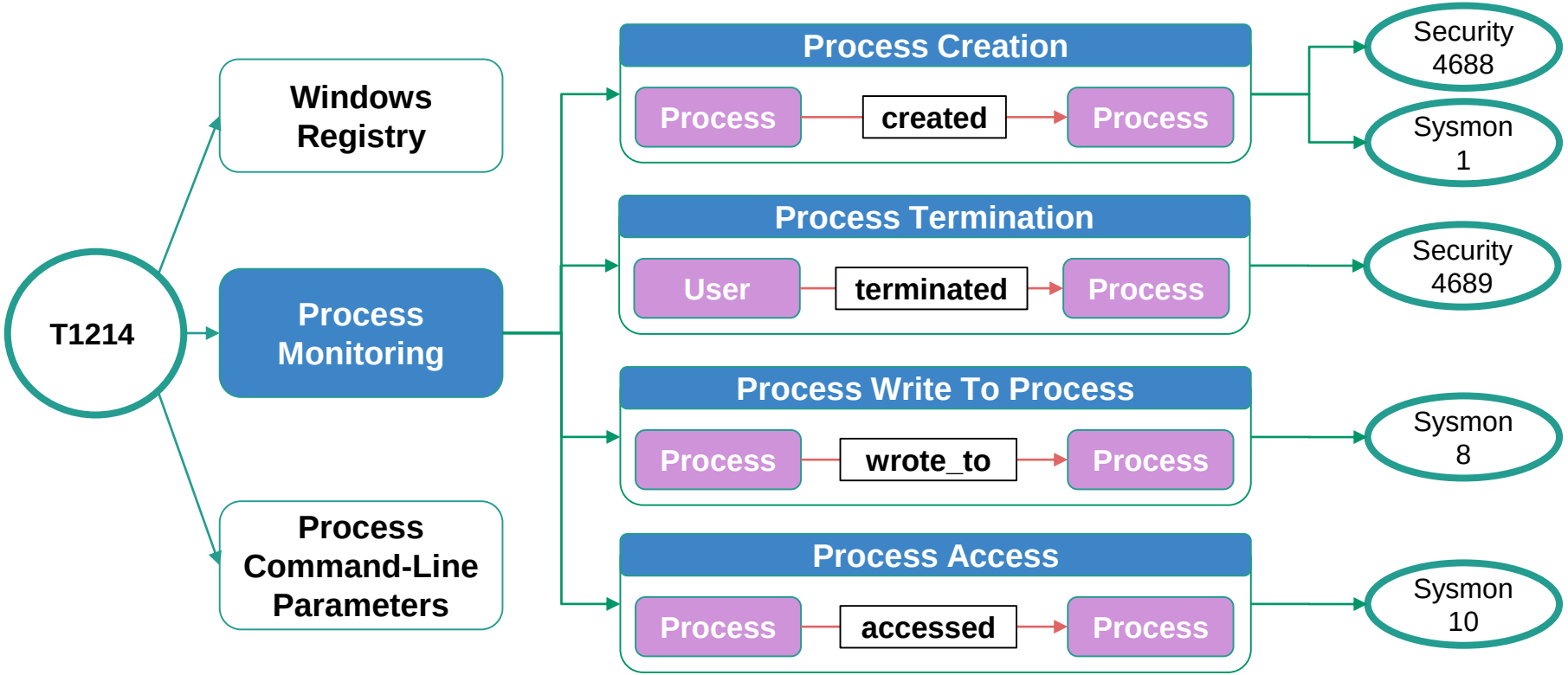


https://github.com/hunters-forge/ATTACK-Python-Client/blob/master/notebooks/ATT%26CK_DataSources.ipynb

ATT&CKing with the right data

ATT&CKcon 2018 Talk!

Credentials in Registry -> DS -> Sub-DS -> Events



https://www.youtube.com/watch?v=QCDBjFJ_C3g

ATT&CK Data (OSSEM-> attack_data_sources)

Data Source	Sub - Data Source	Data Object	Relationship	Data Object	Event ID	Description	Provider Name
File monitoring	file access	user	accessed	file	5145	A network share object was checked to see whether client can be granted desired access	Microsoft-Windows-Security-Auditing
File monitoring	file access request	user	requested_a_handle	file	4656	A handle to an object was requested.	Microsoft-Windows-Security-Auditing
File monitoring	file deletion request	user	requested_a_handle	file	4656	A handle to an object was requested.	Microsoft-Windows-Security-Auditing
File monitoring	file access	user	accessed	file	4663	An attempt was made to access an object.	Microsoft-Windows-Security-Auditing
File monitoring	file deletion	user	deleted	file	4663	An attempt was made to access an object.	Microsoft-Windows-Security-Auditing
File monitoring	file permissions change	user	changed_permissions	file	4670	Permissions on an object were changed.	Microsoft-Windows-Security-Auditing
Loaded DLLs	module load	process	loaded	module	7	The image loaded event logs when a module is loaded in a specific process .	Microsoft-Windows-Sysmon
Named Pipes	win pipe creation	process	created	pipe	17	This event generates when a named pipe is created.	Microsoft-Windows-Sysmon
Named Pipes	win pipe connection	process	connected_to	pipe	18	This event logs when a named pipe connection is made between a client and a server.	Microsoft-Windows-Sysmon
Process monitoring	process creation	process	created	process	4688	A new process has been created	Microsoft-Windows-Security-Auditing
Process monitoring	process creation	process	created	process	1	Process creation	Microsoft-Windows-Sysmon
Process monitoring	process termination	process	terminated	process	4689	A process has exited	Microsoft-Windows-Security-Auditing
Process monitoring	process termination	process	terminated	process	5	The process terminate event reports when a process terminates.	Microsoft-Windows-Sysmon
Process monitoring	process write to process	process	wrote_to	process	8	The CreateRemoteThread event detects when a process creates a thread in another process.	Microsoft-Windows-Sysmon
Process monitoring	process access	process	opened	process	10	The process accessed event reports when a process opens another process.	Microsoft-Windows-Sysmon
Process use of network	process network connection allow	process	connected_to	ip	3	The network connection event logs TCP/UDP connections on the machine.	Microsoft-Windows-Sysmon
Process use of network	process network connection allow	process	connected_to	host	3	The network connection event logs TCP/UDP connections on the machine.	Microsoft-Windows-Sysmon

https://github.com/hunters-forge/OSSEM

A lot more to do..

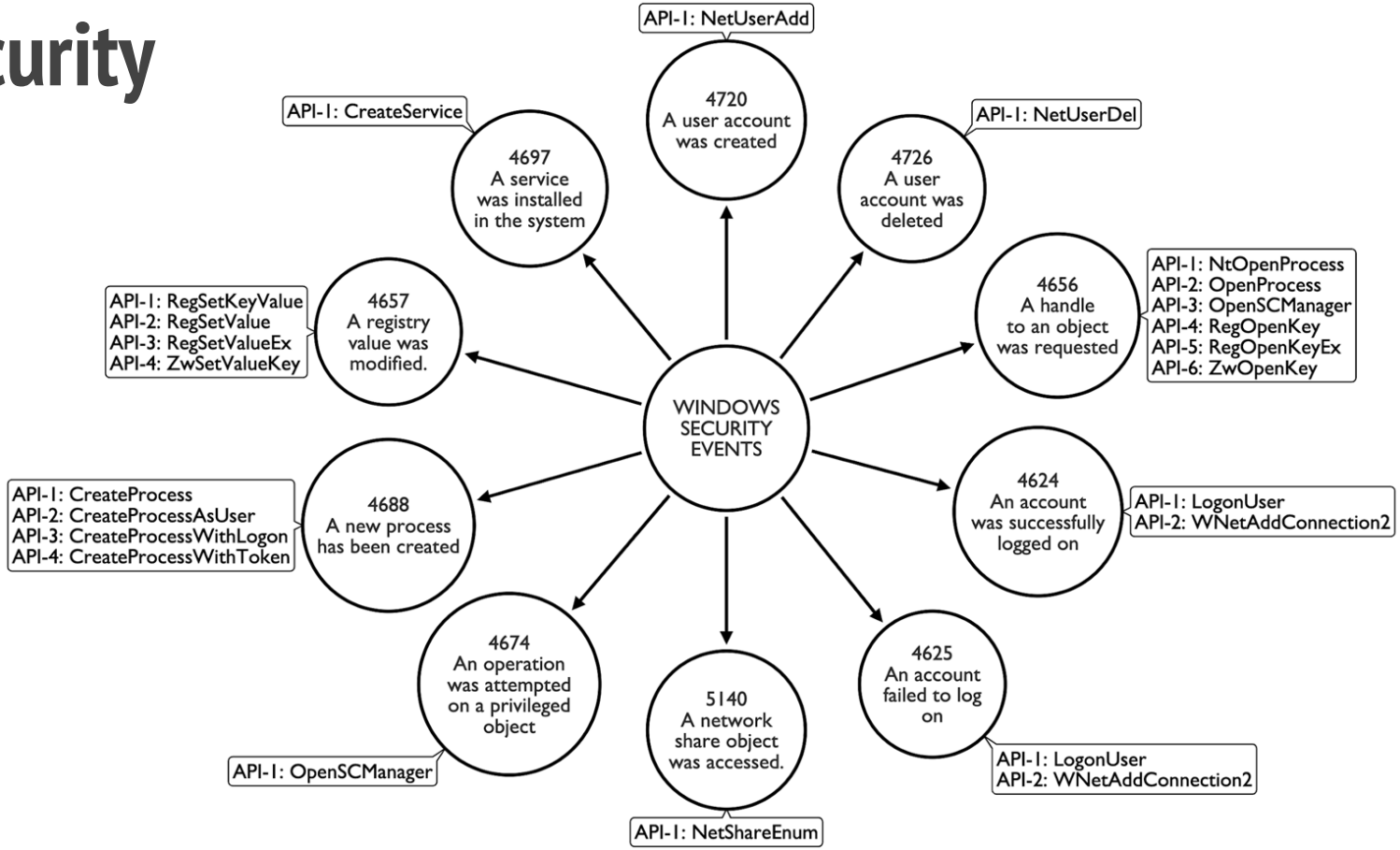
Going deeper!

API-To-Event Project (Windows Security)

API Call	EventID	Event Name	Log Provider	ATT&CK Data Source
LogonUserA	4624	An account was successfully logged on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserExA	4624	An account was successfully logged on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserExW	4624	An account was successfully logged on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserW	4624	An account was successfully logged on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
WNetAddConnection2	4624	An account was successfully logged on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserA	4625	An account failed to log on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserExA	4625	An account failed to log on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserExW	4625	An account failed to log on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
LogonUserW	4625	An account failed to log on	Microsoft-Windows-Security-Auditing	Windows event logs, Authentication logs
NtOpenProcess	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	process monitoring
OpenProcess	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	process monitoring
OpenSCManagerA	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	file monitoring
OpenSCManagerW	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	file monitoring
RegOpenKeyA	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	Windows Registry
RegOpenKeyExA	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	Windows Registry
RegOpenKeyExA	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	Windows Registry
RegOpenKeyExW	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	Windows Registry
ZwOpenKey	4656	A handle to an object was requested	Microsoft-Windows-Security-Auditing	Windows Registry

https://github.com/hunters-forge/API-To-Event

Security



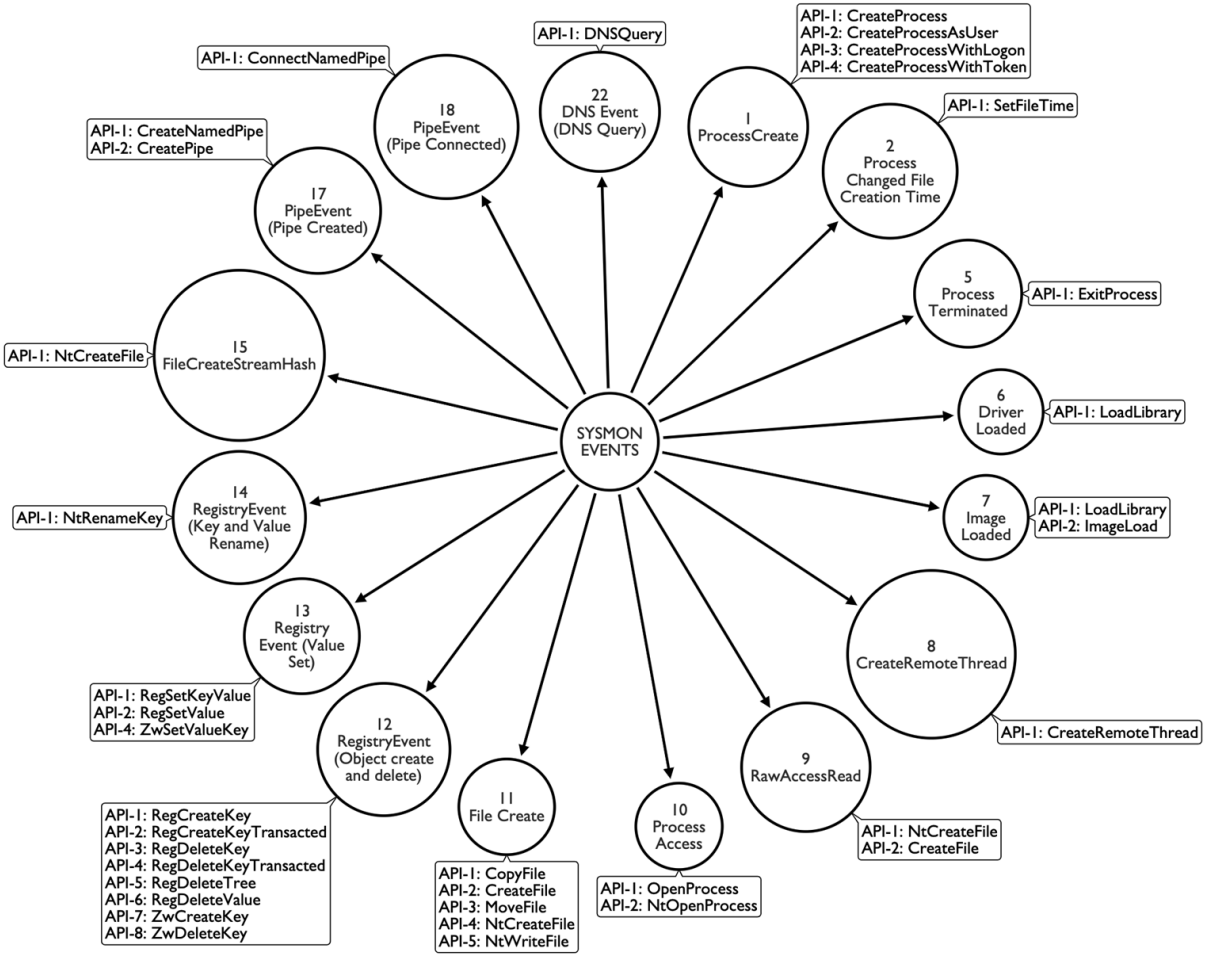
https://github.com/hunters-forge/API-To-Event

API-To-Event Project (Windows Sysmon)

API Call	EventID	Event Name	Log Provider	ATT&CK Data Source
CreateProcessA	1	Process Creation	Microsoft-Windows-Sysmon	Process monitoring
CreateProcessAsUserA	1	Process Creation	Microsoft-Windows-Sysmon	Process monitoring
CreateProcessAsUserW	1	Process Creation	Microsoft-Windows-Sysmon	Process monitoring
CreateProcessW	1	Process Creation	Microsoft-Windows-Sysmon	Process monitoring
CreateProcessWithLogonW	1	Process Creation	Microsoft-Windows-Sysmon	Process monitoring
CreateProcessWithTokenW	1	Process Creation	Microsoft-Windows-Sysmon	Process monitoring
OpenProcess	10	ProcessAccess	Microsoft-Windows-Sysmon	process monitoring
NtOpenProcess	10	ProcessAccess	Microsoft-Windows-Sysmon	process monitoring
CopyFile	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
CopyFile2	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
CopyFileEx	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
CreateFile2	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
CreateFileA	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
CreateFileW	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
MoveFile	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
NtCreateFile	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
NtWriteFile	11	FileCreate	Microsoft-Windows-Sysmon	file monitoring
RegCreateKeyA	12	RegistryEvent (Object create and delete)	Microsoft-Windows-Sysmon	Windows Registry

https://github.com/hunters-forge/API-To-Event

Sysmon



https://github.com/hunters-forge/API-To-Event

A few opportunities!

Exploring Data Sources 2.0!

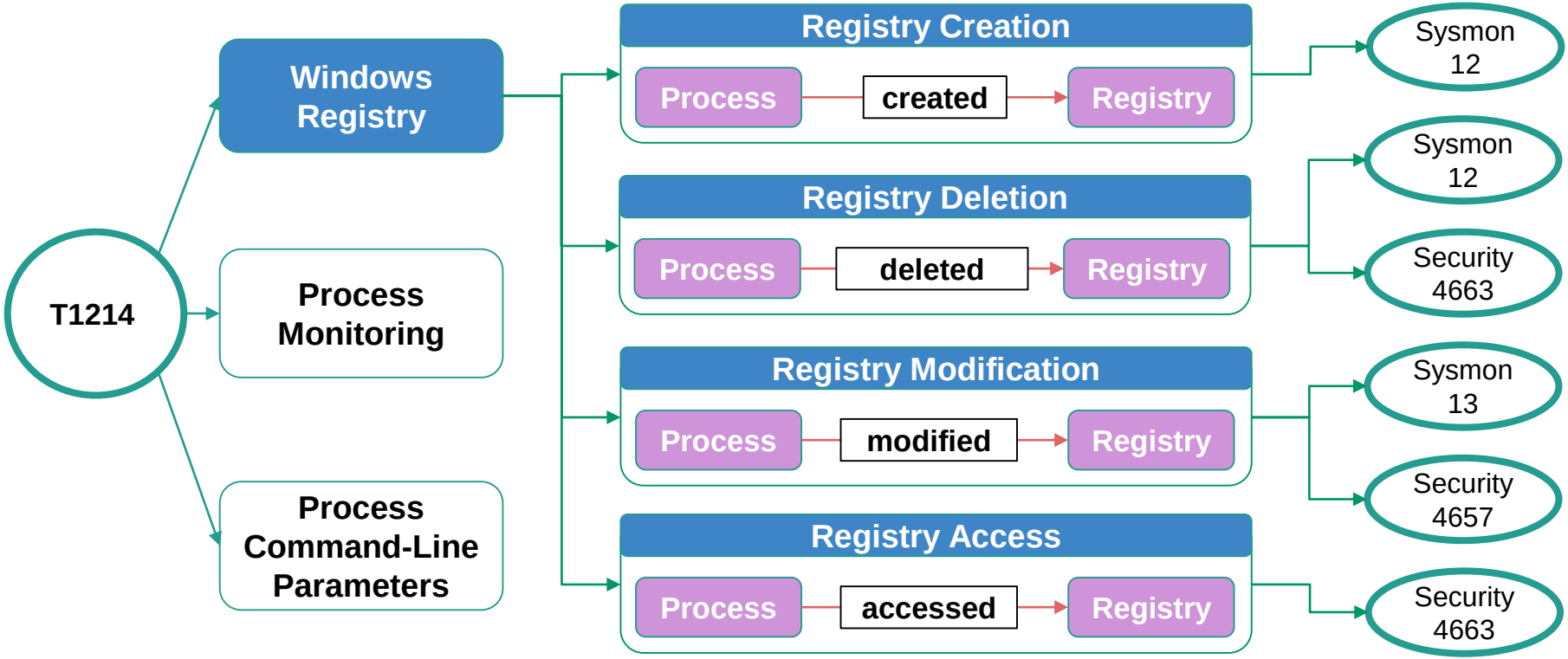
A few opportunities..

- ATT&CK Data sources covered by other data sources
- Windows Event Logs data source is too broad!
- ATT&CK data sources and the wrong platforms!
- Validation of ATT&CK data sources recommendations
  - What specific event logs per data source?

A few opportunities!

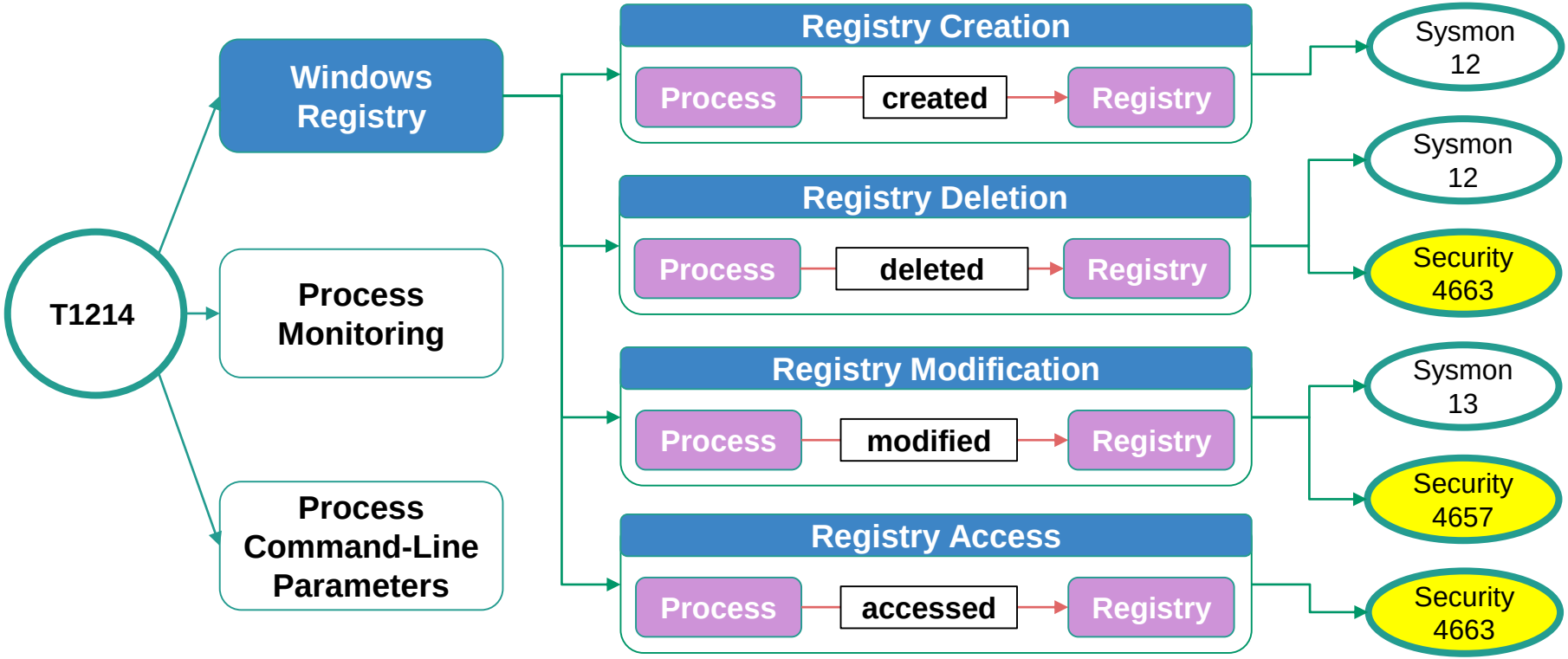
- ATT&CK Data sources covered by other data sources
- Windows Event Logs data source is too broad!

Credentials in Registry - Windows Registry



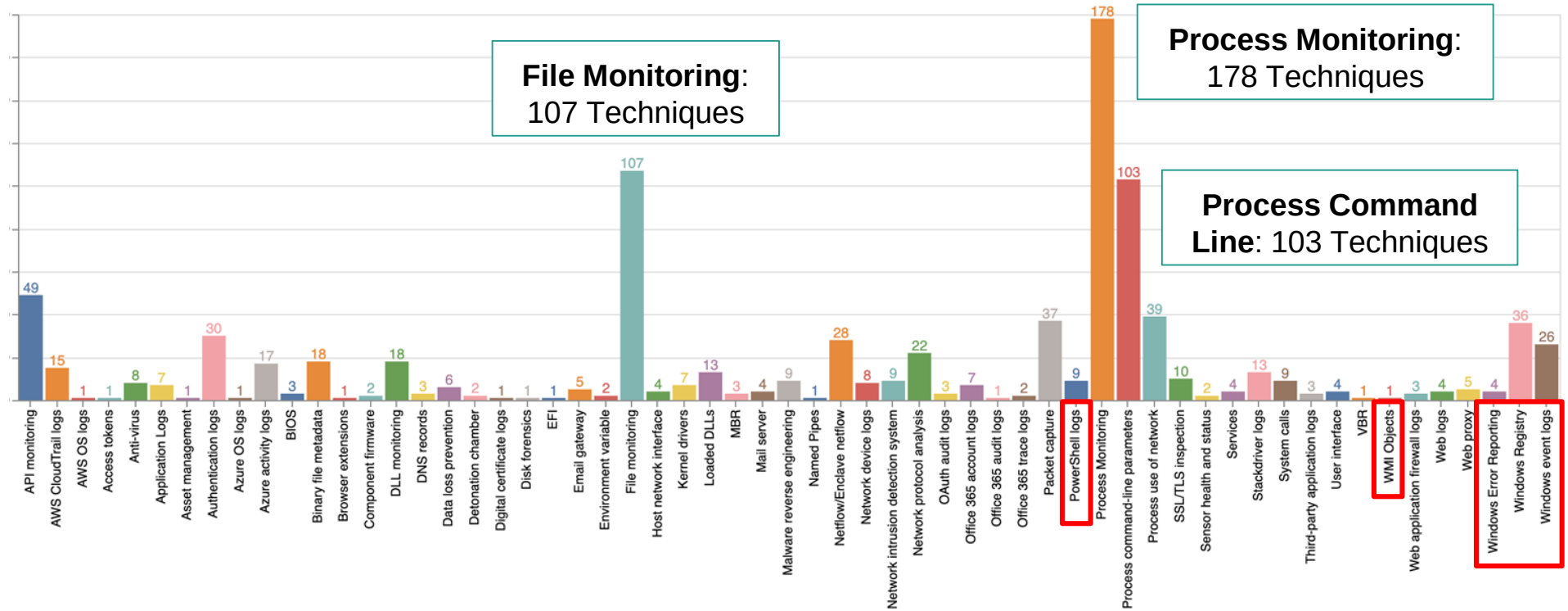
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Registry & Windows Security Event Logs?



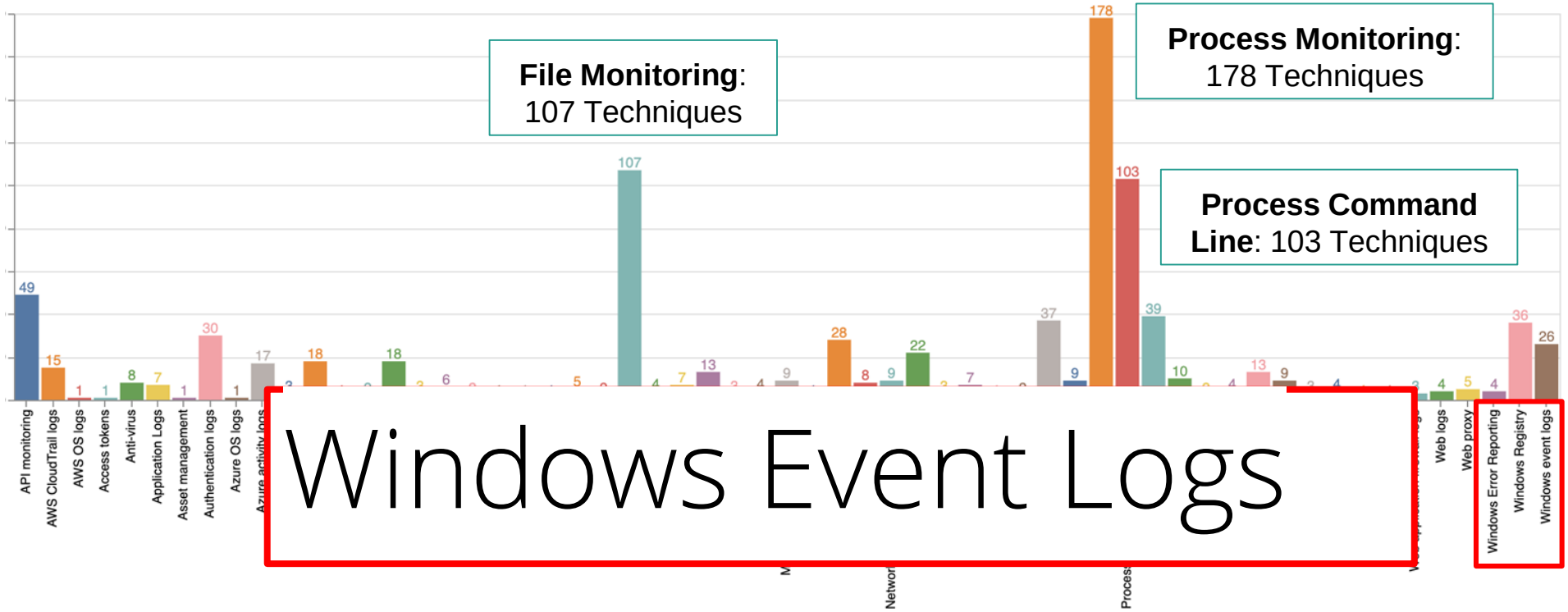
https://www.youtube.com/watch?v=QCDBjFJ_C3g

ATT&CK Techniques with Data Sources (265)

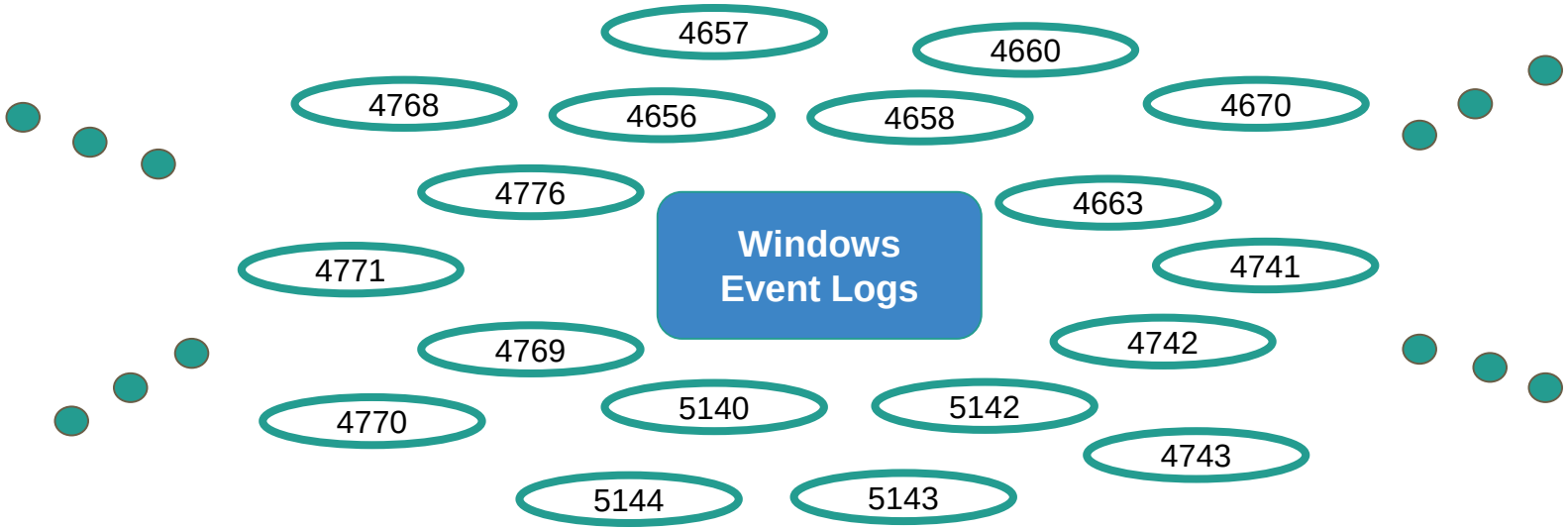


https://github.com/hunters-forge/ATTACK-Python-Client/blob/master/notebooks/ATT%26CK_DataSources.ipynb

ATT&CK Techniques with Data Sources (265)

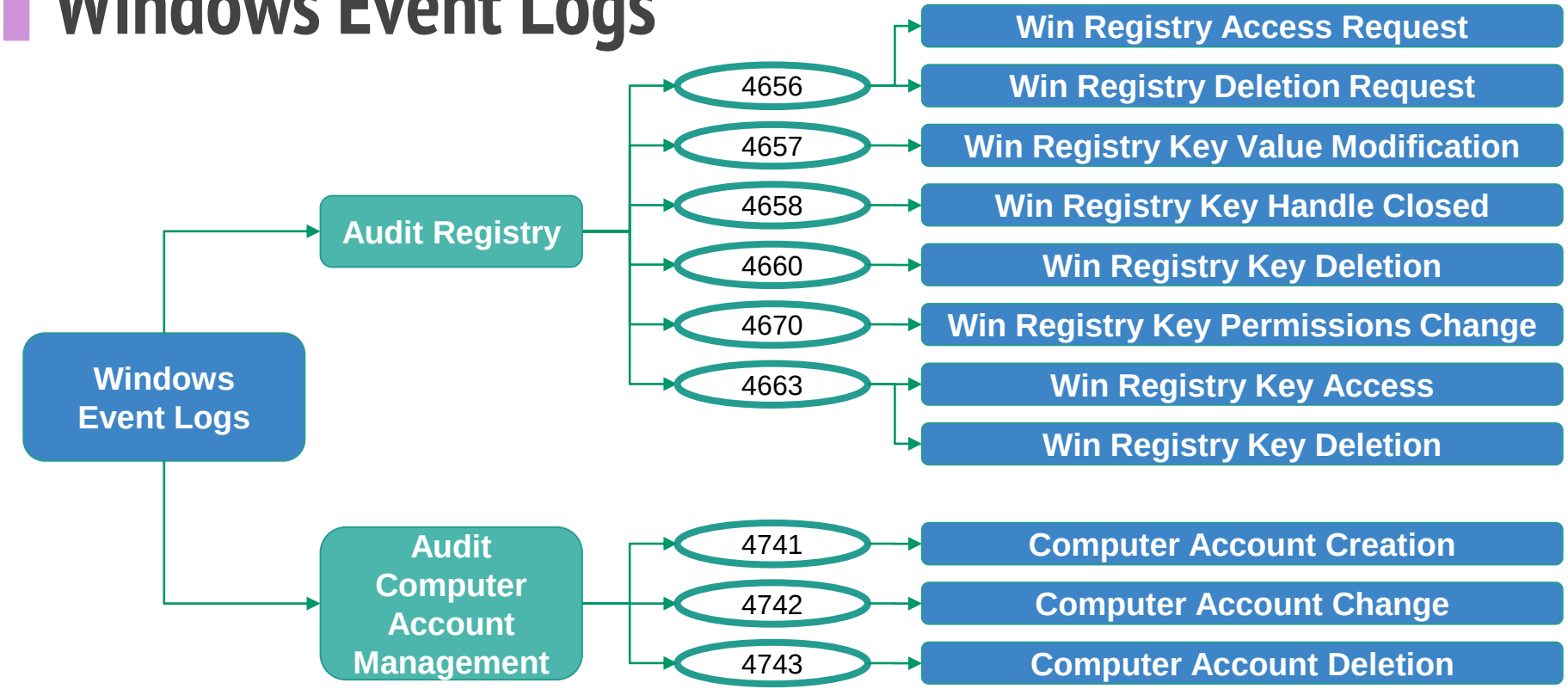


Windows Event Logs … a Universe Behind?



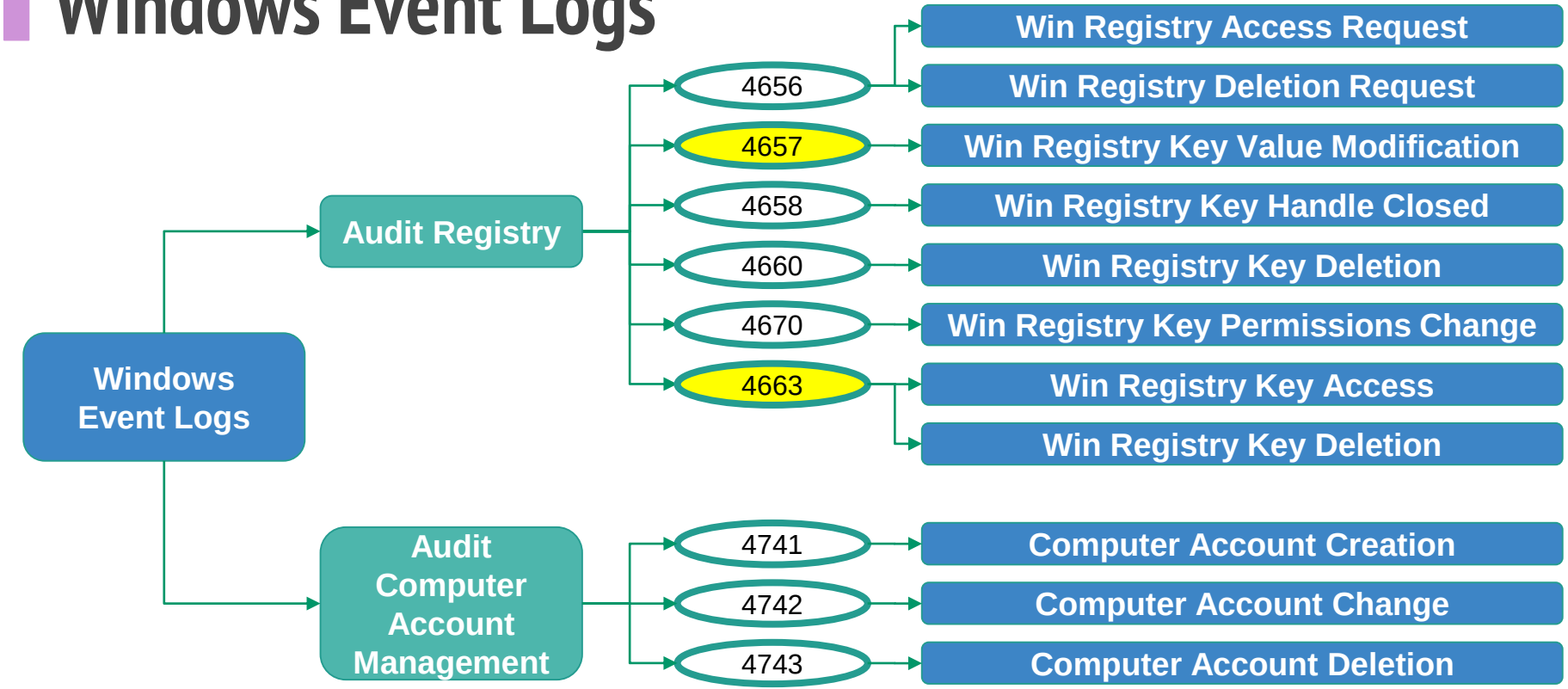
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Event Logs



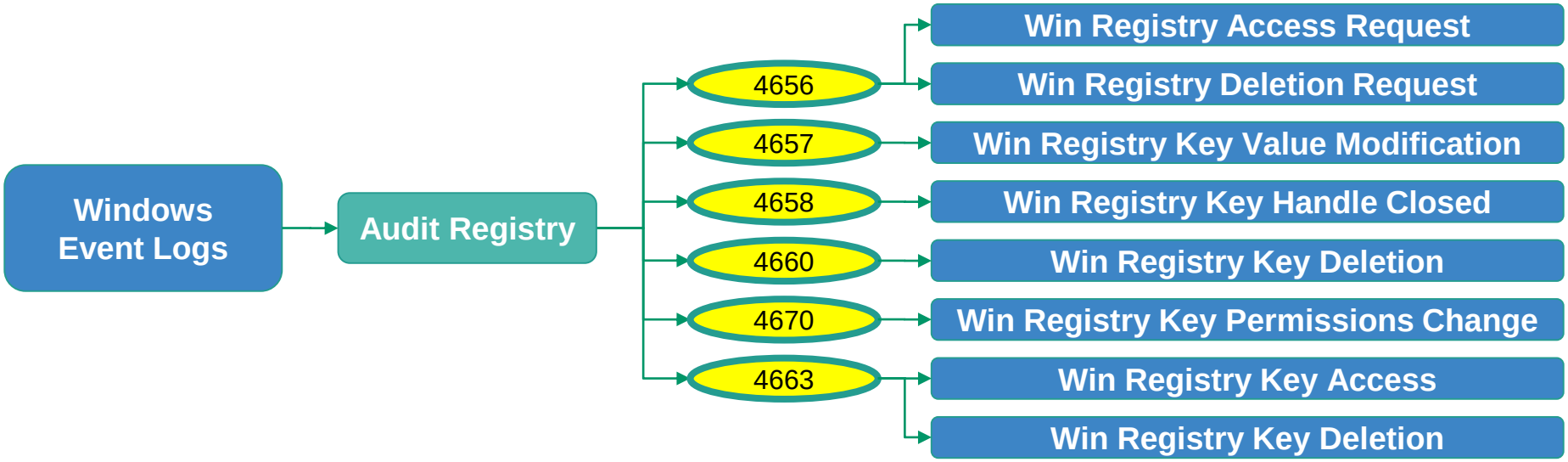
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Event Logs



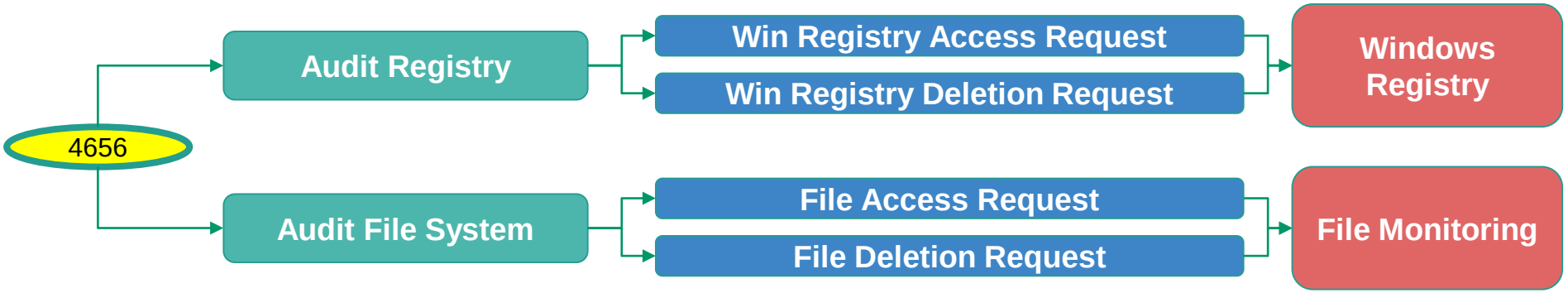
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Event Logs



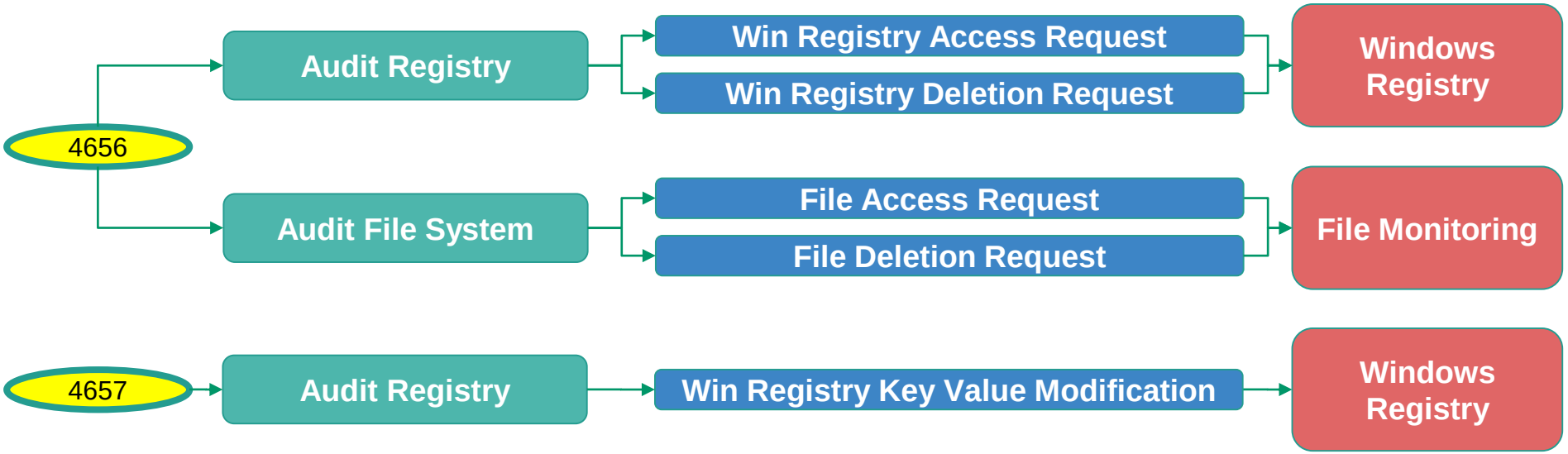
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Event Log 4656: A handle to an object was requested



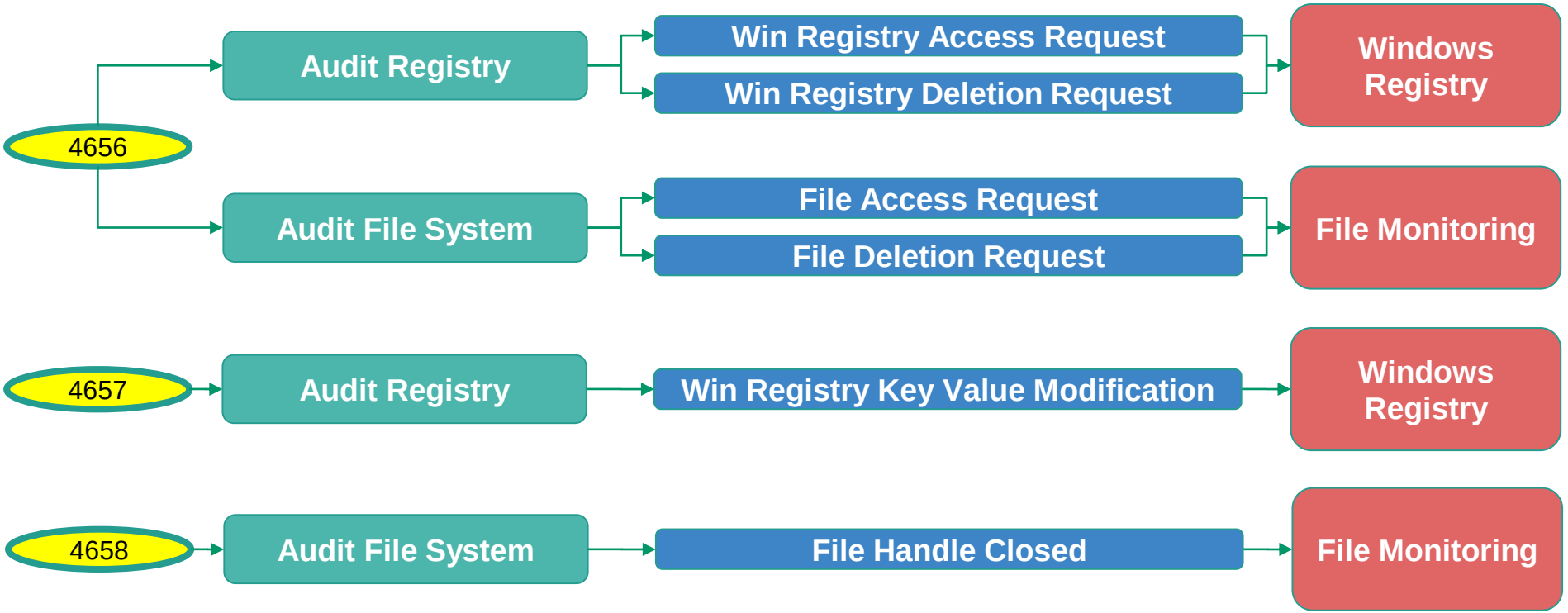
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Event Log 4657: A registry value was modified



https://www.youtube.com/watch?v=QCDBjFJ_C3g

Windows Event Log 4658: The handle to an object was closed



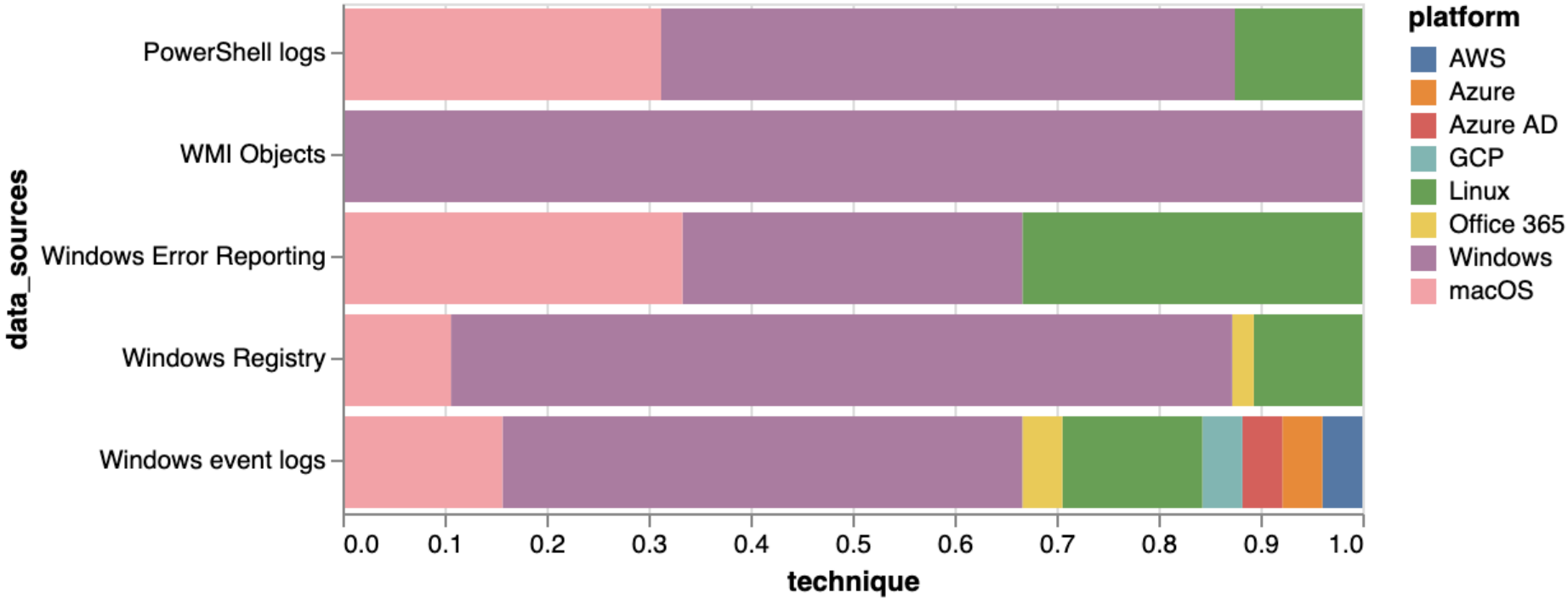
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Currently collaborating with ATT&CK team..

A few opportunities!

ATT&CK data sources and the wrong platforms!

ATT&CK Windows Data Sources & Platform (2019)

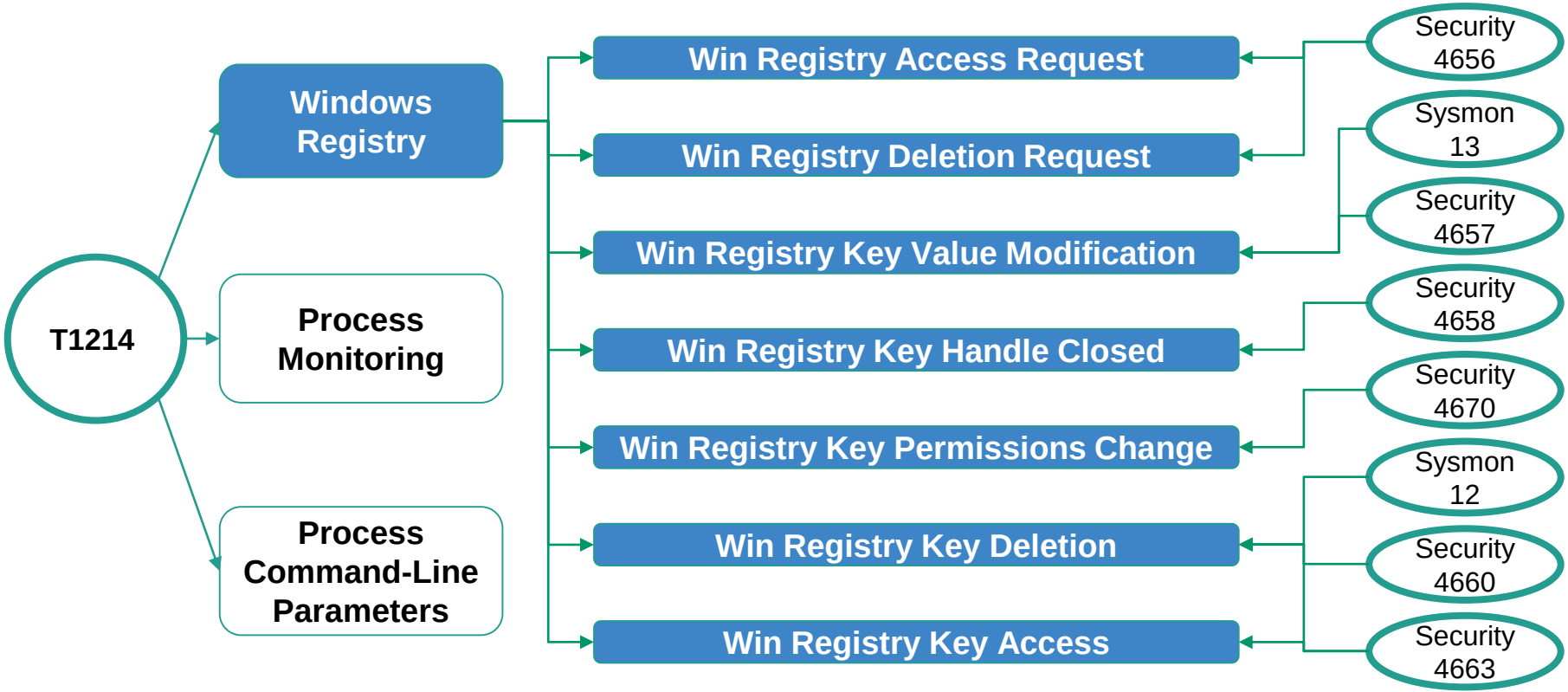


https://github.com/hunters-forge/ATTACK-Python-Client/blob/master/notebooks/ATT%26CK_DataSources.ipynb

A few opportunities!

- Validation of ATT&CK data sources recommendations
  - What specific event logs per data source?

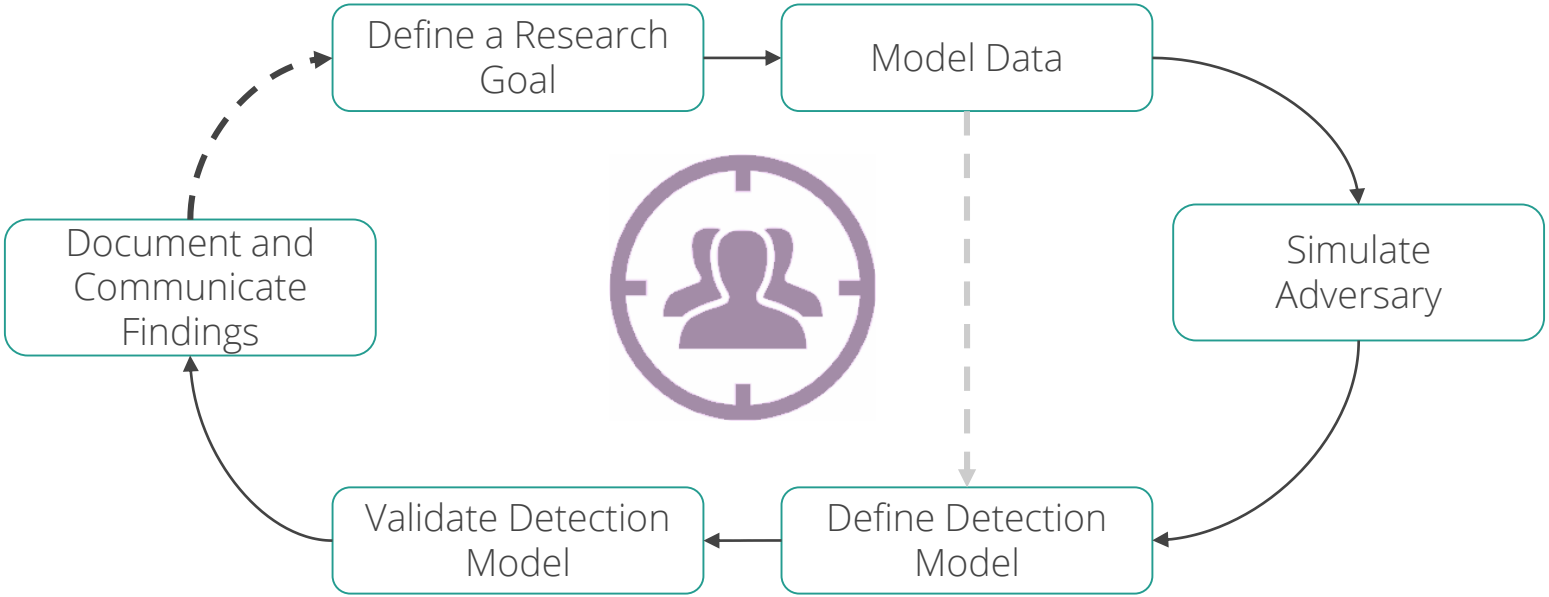
Credentials in Registry - Windows Registry



https://www.youtube.com/watch?v=QCDBjFJ_C3g

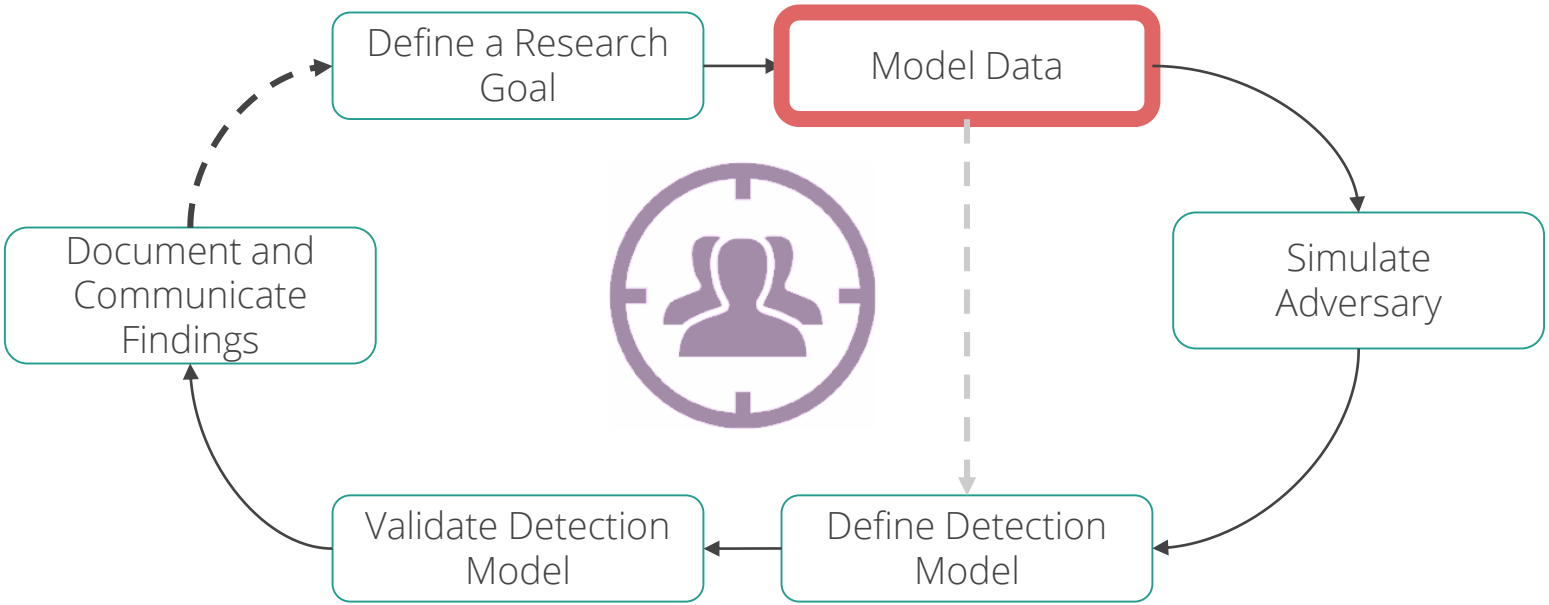
Wait! Where is all this happening so far?

Data Analytics Development (Example)



https://www.youtube.com/watch?v=DuUF-zXUzPs

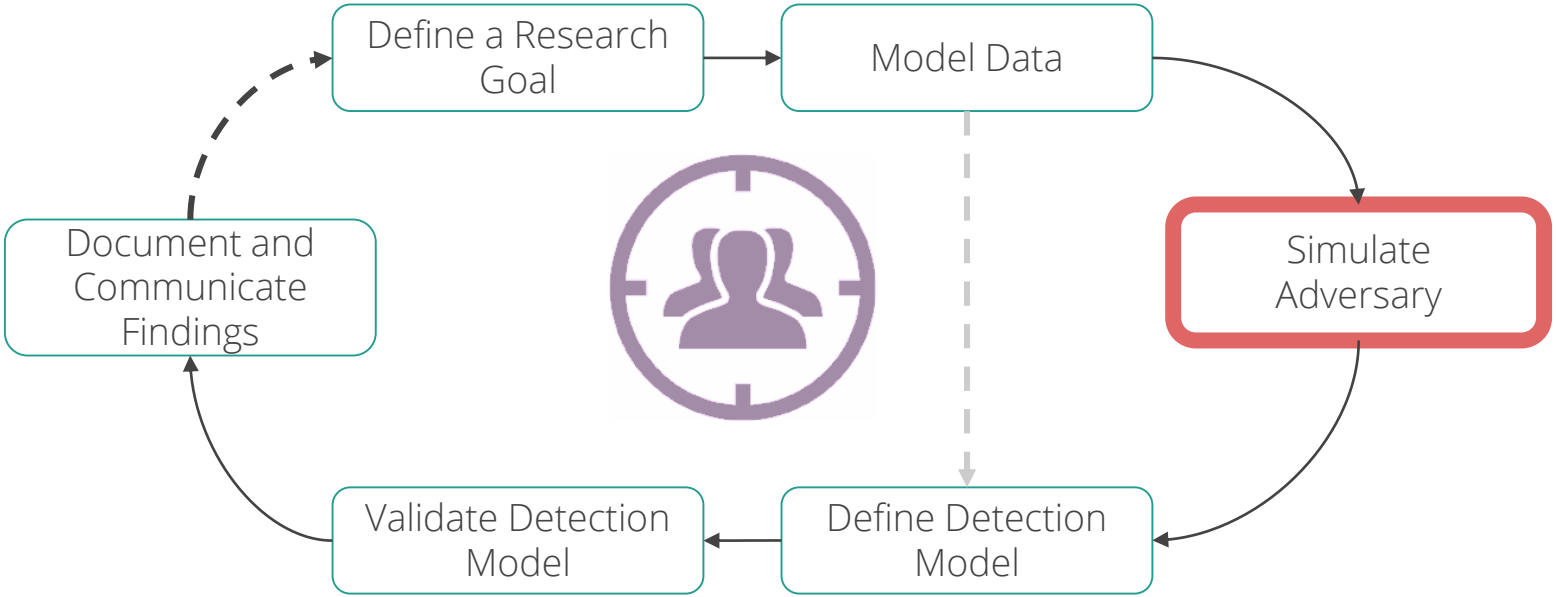
Data Analytics Development (Example)



https://www.youtube.com/watch?v=DuUF-zXUzPs

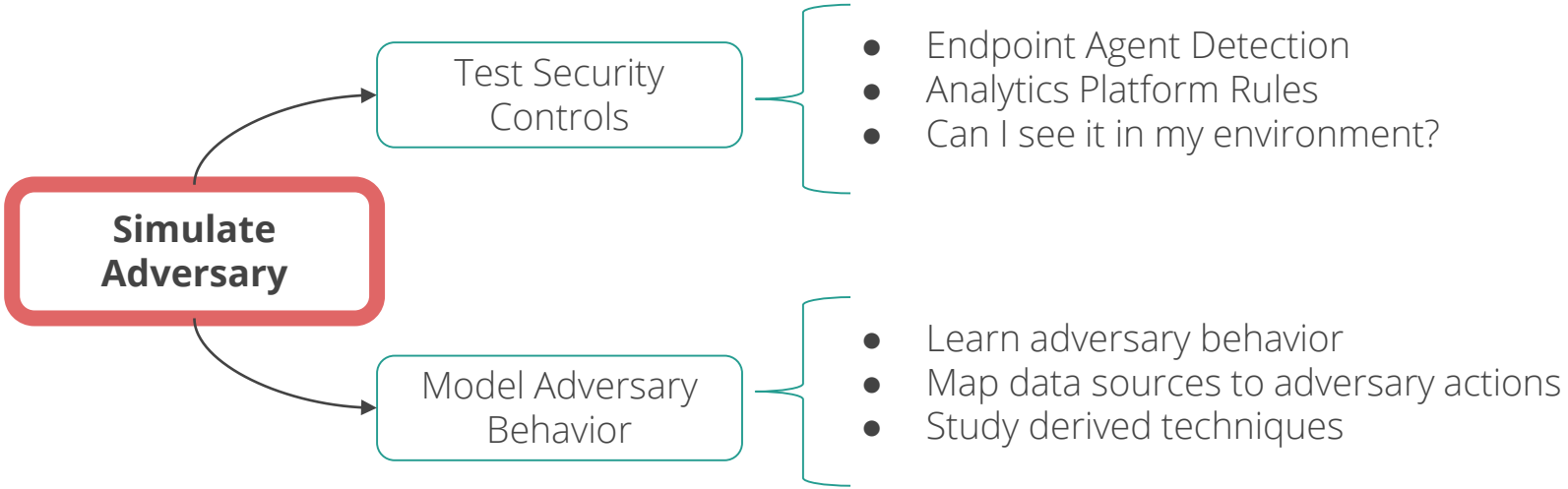
How do we validate our data recommendations?

Data Analytics Development (Example)

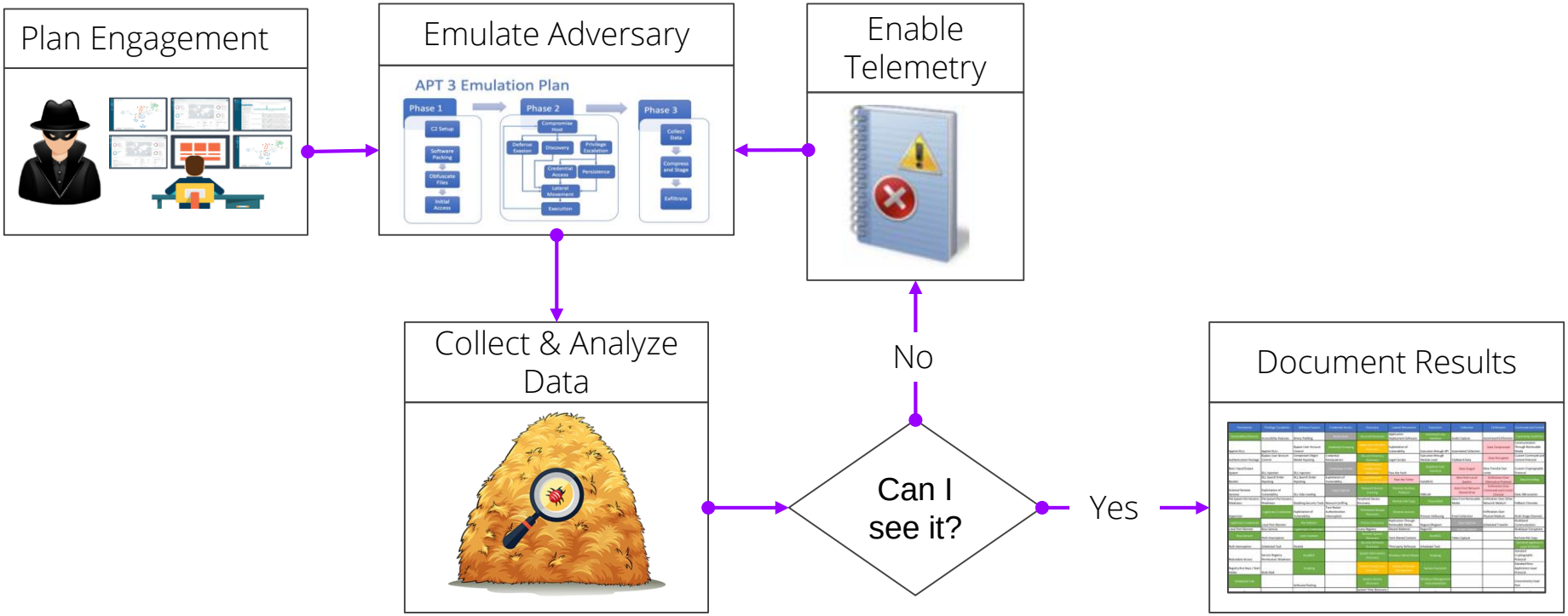


https://www.youtube.com/watch?v=DuUF-zXUzPs

More than just testing security controls!



A basic adversary simulation flow!



What do we need for Credentials in Registry?

Credentials in Registry

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: [1]

- Local Machine Hive: `reg query HKLM /f password /t REG_SZ /s`
- Current User Hive: `reg query HKCU /f password /t REG_SZ /s`

ID: T1214

Tactic: Credential Access

Platform: Windows

System Requirements: Ability to query some Registry locations depends on the adversary's level of access. User permissions are usually limited to access of user-related Registry keys.

Permissions Required: User, Administrator

Data Sources: Windows Registry, Process command-line parameters, Process monitoring

Contributors: Sudhanshu Chauhan, @Sudhanshu_C

Version: 1.0

https://attack.mitre.org/techniques/T1214/

What do we need for Credentials in Registry?

Credentials in Registry

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: [1]

- Local Machine Hive: `reg query HKLM /f password /t REG_SZ /s`
- Current User Hive: `reg query HKCU /f password /t REG_SZ /s`

ID: T1214

Tactic: Credential Access

Platform: Windows

System Requirements: Ability to query some Registry locations depends on the adversary's level of access. User permissions are usually limited to access of user-related Registry keys.

Permissions Required: User, Administrator

Data Sources: Windows Registry, Process command-line parameters, Process monitoring

Contributors: Sudhanshu Chauhan, @Sudhanshu_C

Version: 1.0

https://attack.mitre.org/techniques/T1214/

What else do we need for Credentials in Registry?

- Windows Registry?
  - Enable Audit Object Access > Audit Registry
- Process Monitoring?
  - Enable Audit Detailed Tracking > Audit Process Creation
- Process Command-line Parameters?
  - Enable Administrative Templates\System\Audit Process Creation > Include command line in process creation events

What else do we need for Credentials in Registry?

- Windows Registry?
  - Enable Audit Object Access > Audit Registry
  - **Set Audit Rule to trigger event!**
- Process Monitoring?
  - Enable Audit Detailed Tracking > Audit Process Creation
- Process Command-line Parameters?
  - Enable Administrative Templates\System\Audit Process Creation > Include command line in process creation events

https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists

What else do we need for Credentials in Registry?

- What are we testing?
  - Available default automatic logon user Settings!!

```
Set-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name AutoAdminLogon -Value 1

Set-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultUserName -Value pgustavo

Set-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name DefaultPassword -Value W1n1!2019
```

https://github.com/hunters-forge/Blacksmith/blob/master/aws/mordor/cfn-files/scripts/default/Join-Domain.ps1#L37-L49

What else do we need for Credentials in Registry?

- **Set Audit Rule! How?**
  - Download **https://github.com/hunters-forge/Set-AuditRule**
  - Import-module Set-AuditRule.ps1
  - Set-AuditRule -RegistryPath "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -IdentityReference Everyone -Rights QueryValues -InheritanceFlags None -PropagationFlags None -AuditFlags Success

What else do we need for Credentials in Registry?

- **Testing Commands?**
  - reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /f password /t REG_SZ /s

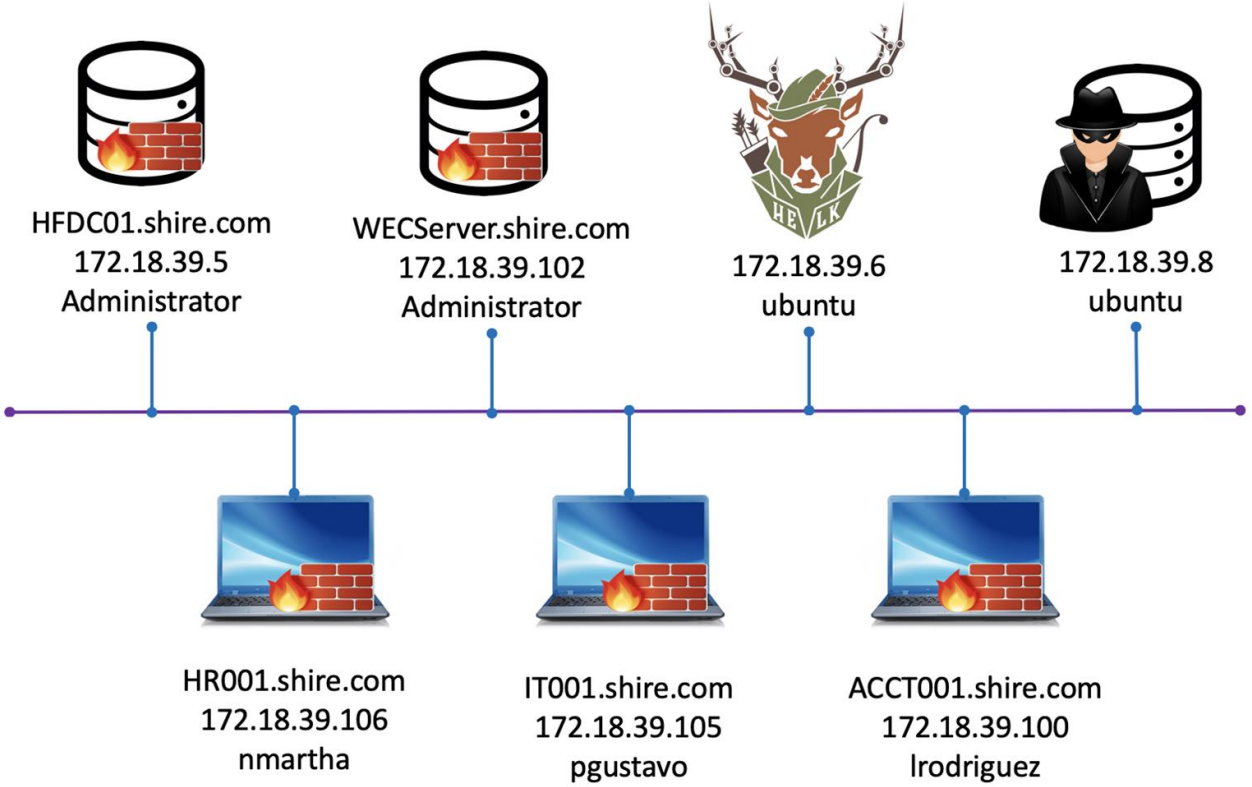
What about technique variations?

What else do we need for Credentials in Registry?

- **Testing Commands?**
  - reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /f password /t REG_SZ /s
  - Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" -Name *password*
  - C#, Python, etc!

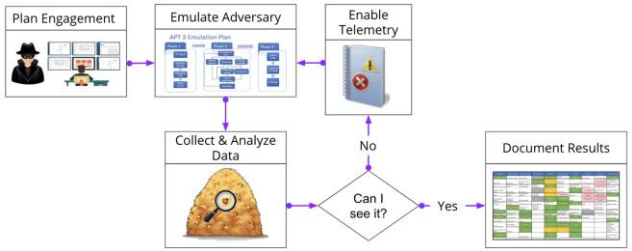
Are we ready?

We need an environment setup.. working!



Execute -> Collect -> Analyze -> Repeat

Simulating Adversarial Technique

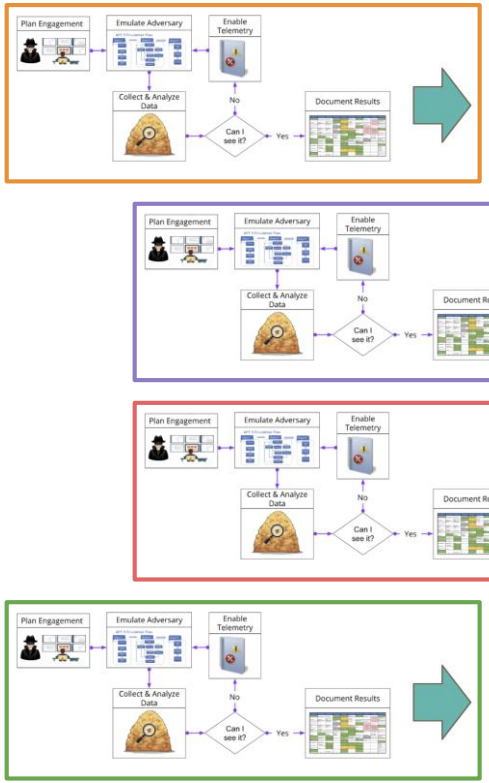


Data produced

Test Security Controls

Model Adversary Behavior

Same Technique + Some Variations



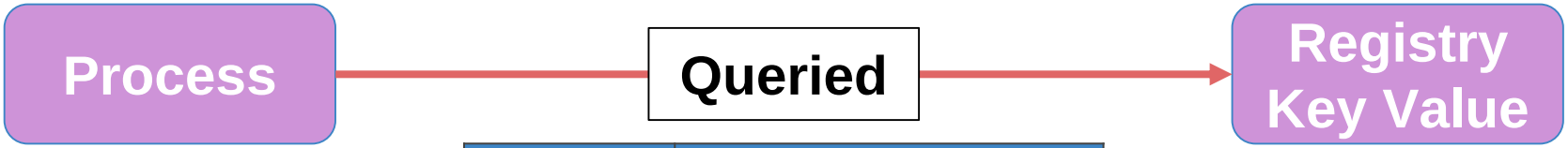
Data produced

Test Security Controls

Model Adversary Behavior

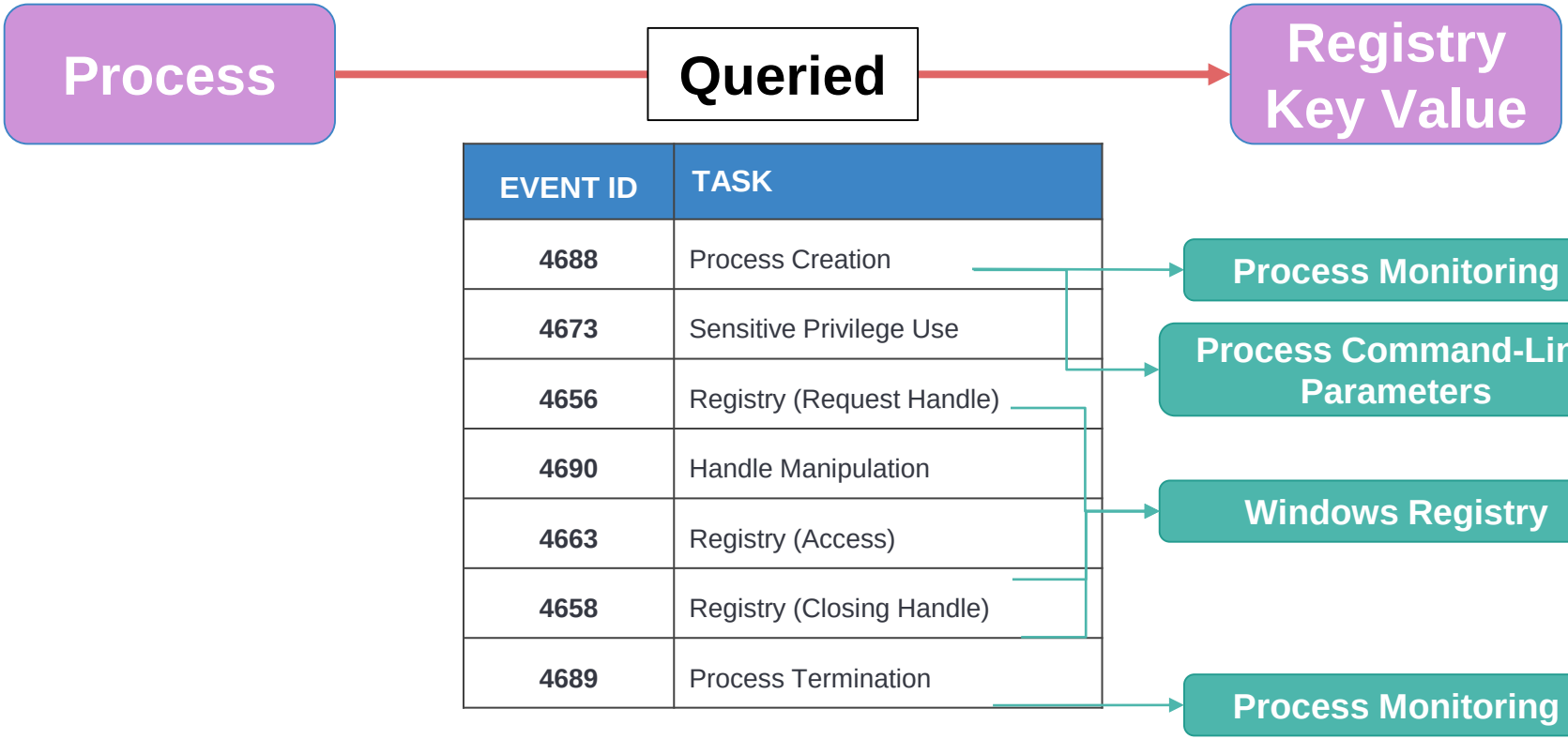
Credentials in Registry Data Mapping

Credentials in Registry Data Mapping

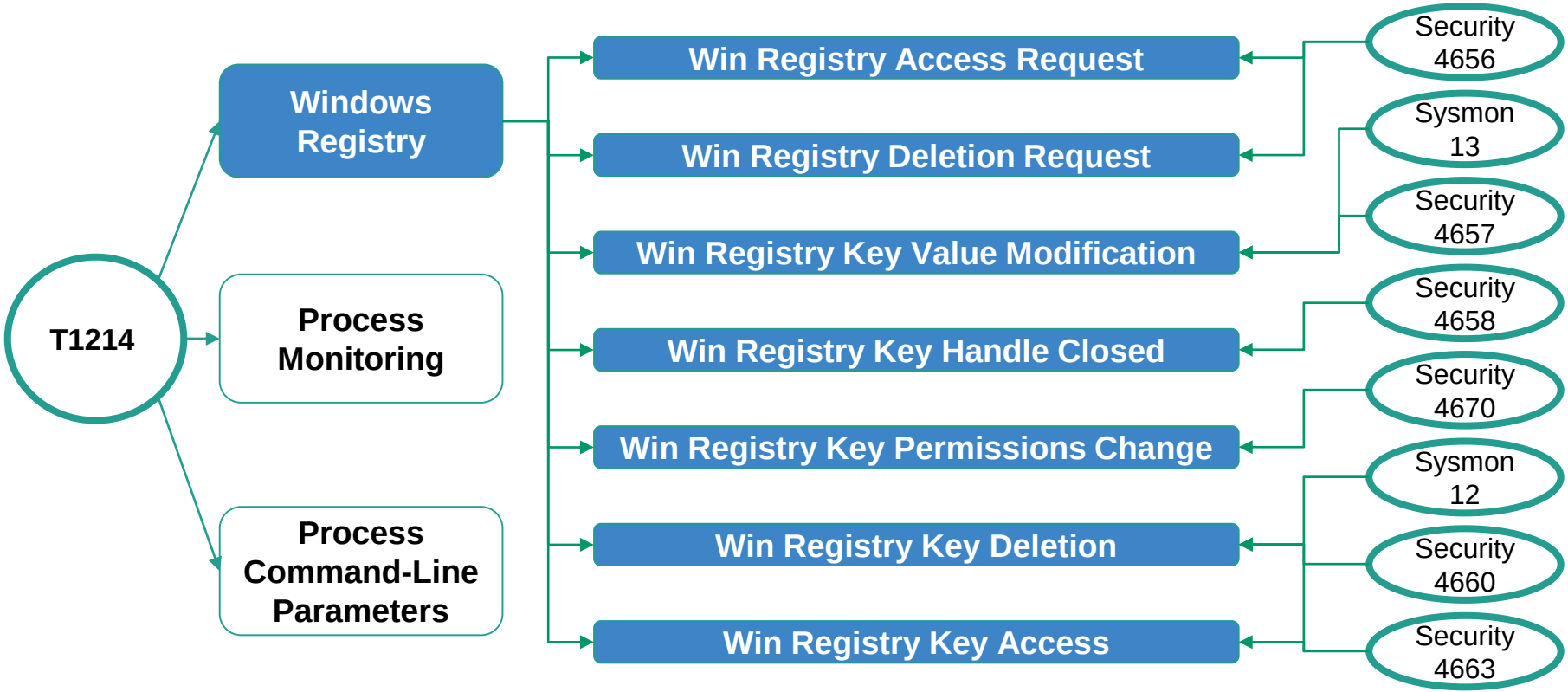


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

Credentials in Registry Data Mapping

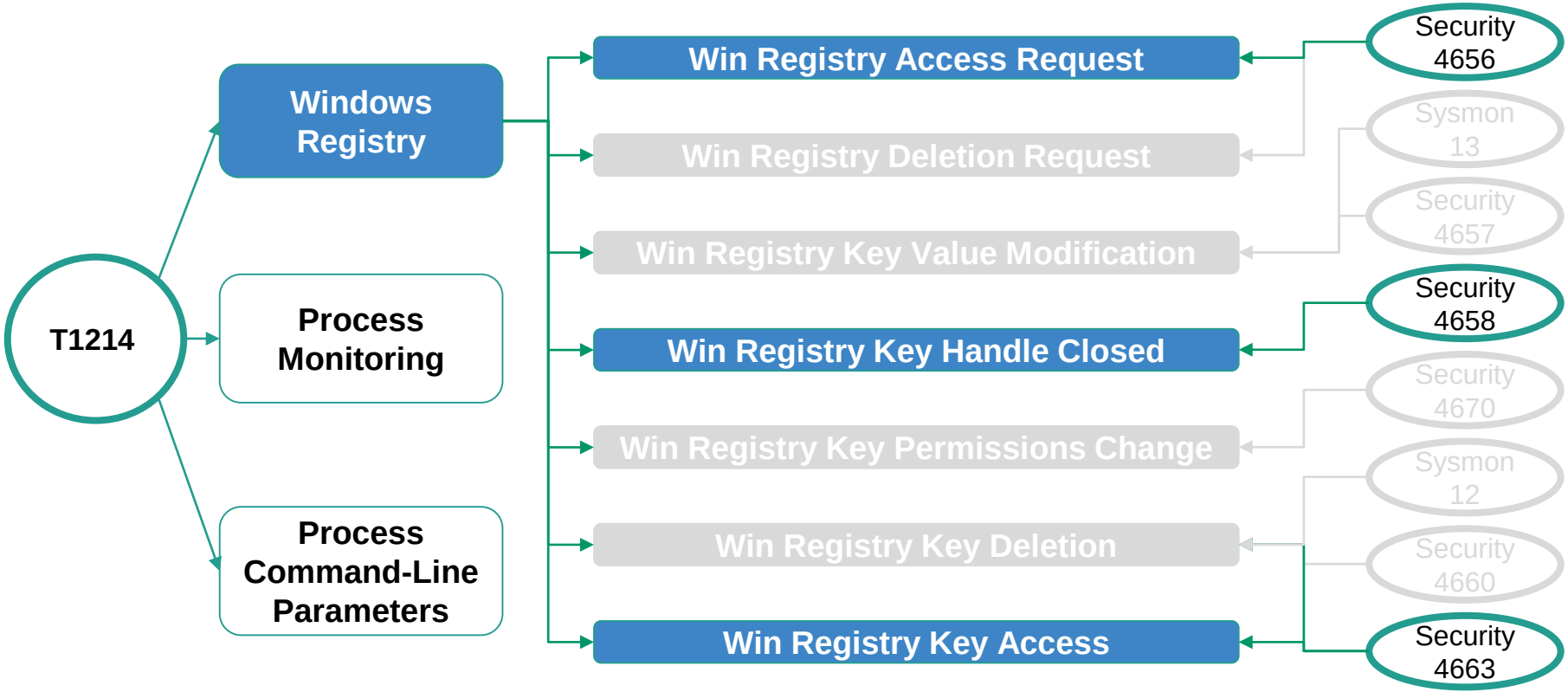


Credentials in Registry - Windows Registry



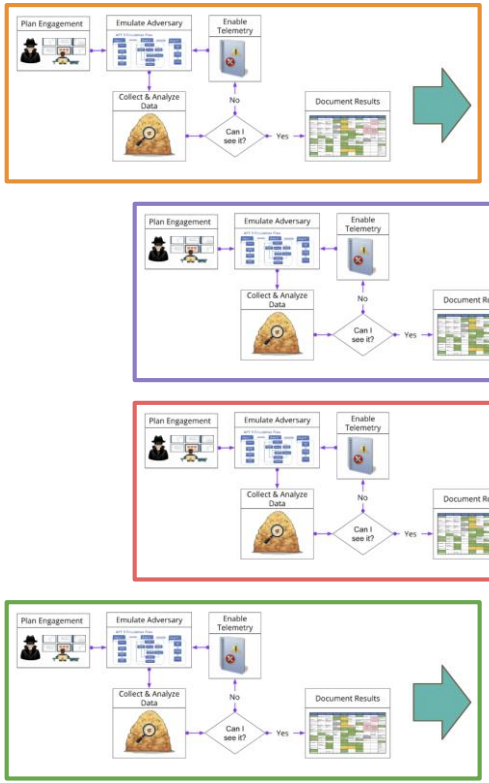
https://www.youtube.com/watch?v=QCDBjFJ_C3g

Credentials in Registry - Windows Registry



https://www.youtube.com/watch?v=QCDBjFJ_C3g

Spending +time producing data & -time analyzing



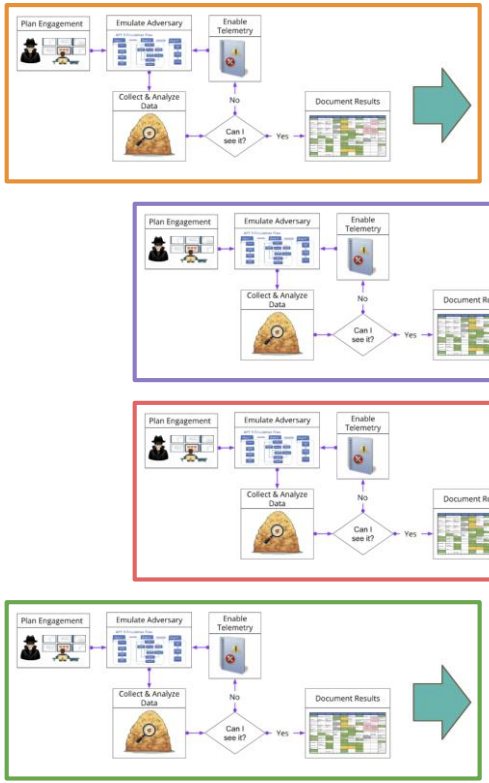
Data produced

Test Security Controls

Model Adversary Behavior

Takes Time!
Similar Events?

Same Technique + Some Variations

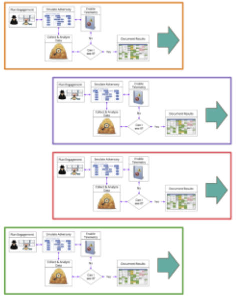


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

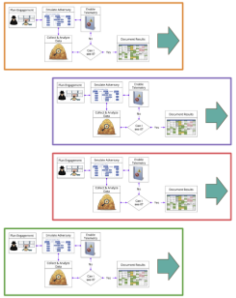
Test Security Controls

Model Adversary Behavior

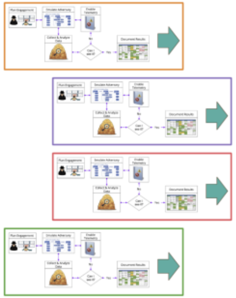
We might be all doing this..



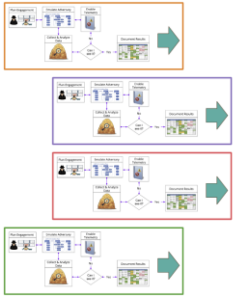
EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination



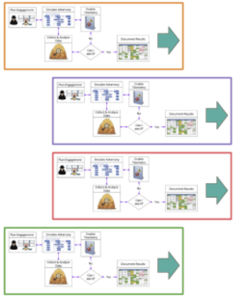
EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination



EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

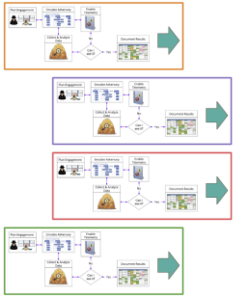


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

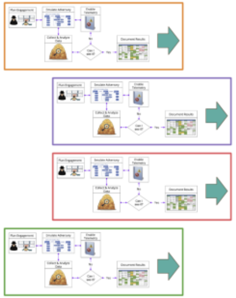


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

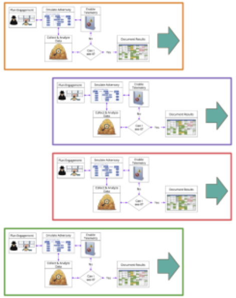
We might be doing this over and over..



EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

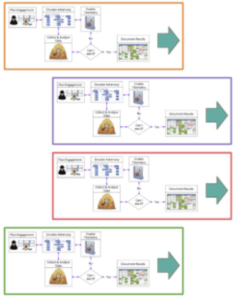


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

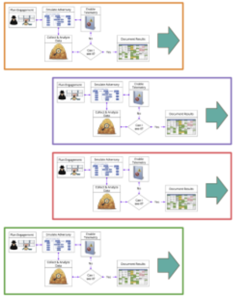


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

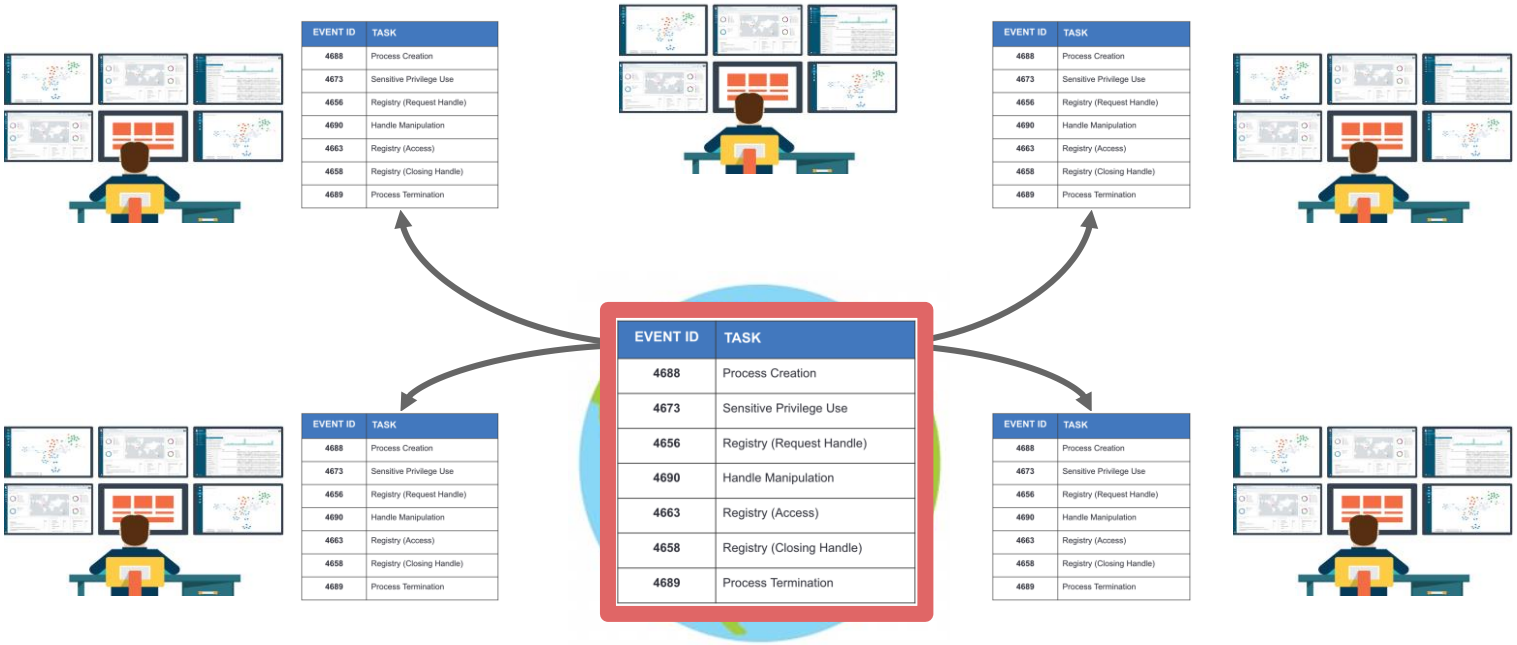


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

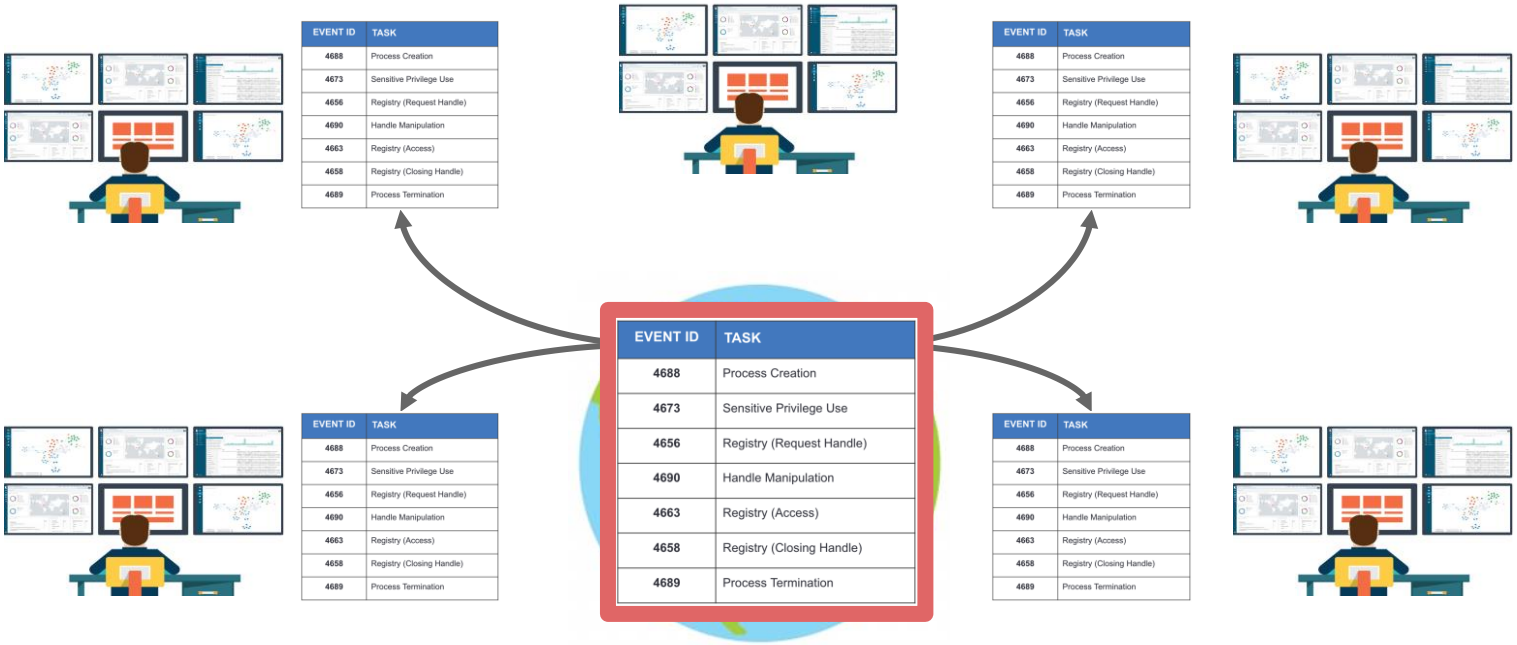


EVENT ID	TASK
4688	Process Creation
4673	Sensitive Privilege Use
4656	Registry (Request Handle)
4690	Handle Manipulation
4663	Registry (Access)
4658	Registry (Closing Handle)
4689	Process Termination

What if we share our datasets?



From Zero to Data Analytics Validation!



Enter Mordor

Mordor Project @Mordor_Project

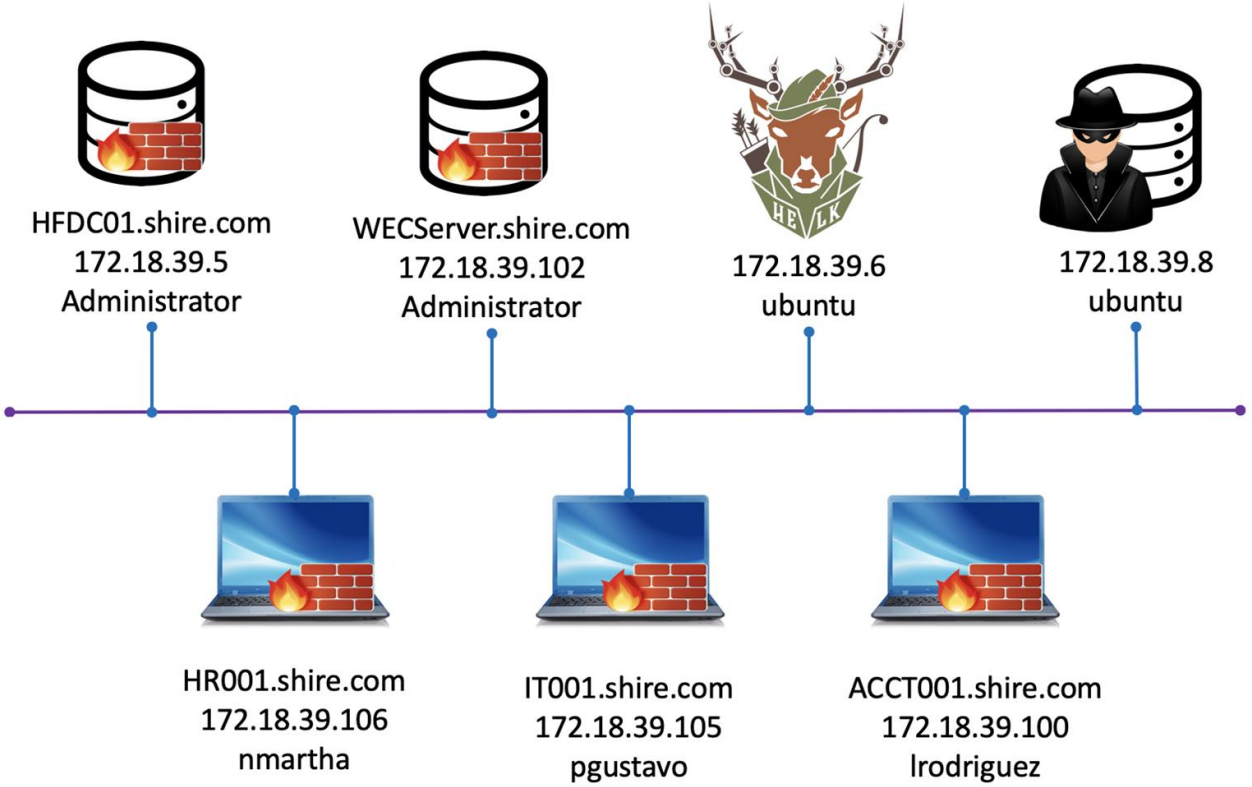
- Pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON)
- Pre-recorded data categorized by platforms, adversary groups, tactics and techniques defined by the Mitre ATT&CK Framework.
- Data represents not only specific known malicious events but additional context/events that occur around it.

Mordor Standard Environments

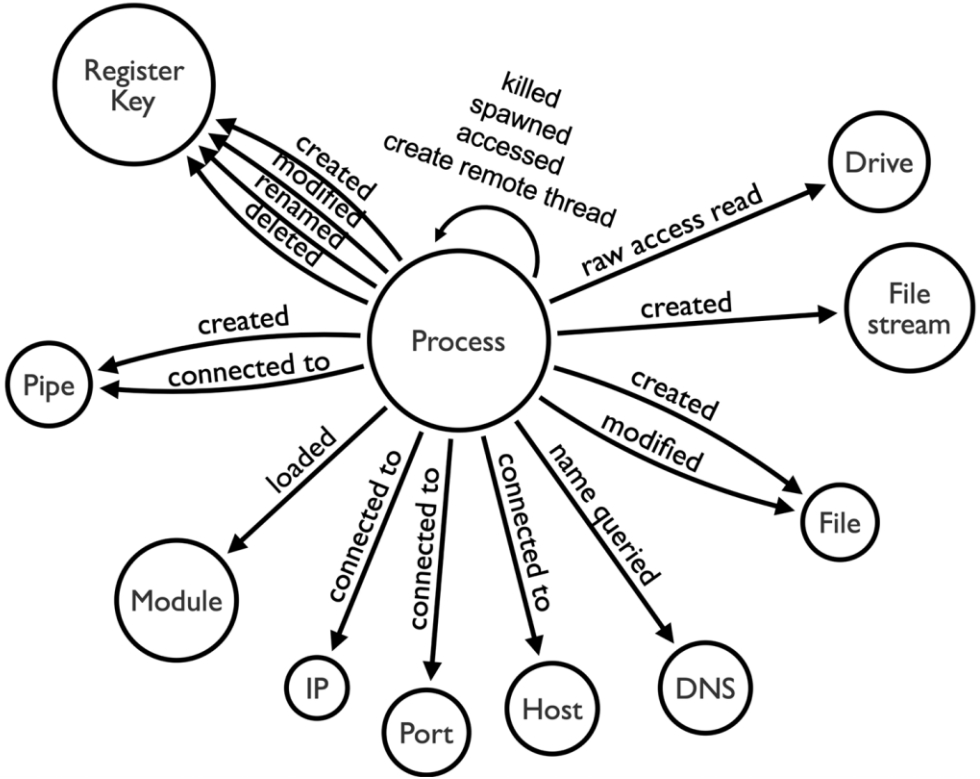
- Environment designed to replicate a small research network
- Standardized and documented setup
- Platforms
  - Windows
  - Linux
- Endpoints Telemetry
  - Windows Security Auditing
  - Event Tracing for Windows (ETW) (NEW!!)
- Network Telemetry
  - Network Logs
- Environments Available: Shire and Erebor

Mordor Environments: The Shire

The Shire Design

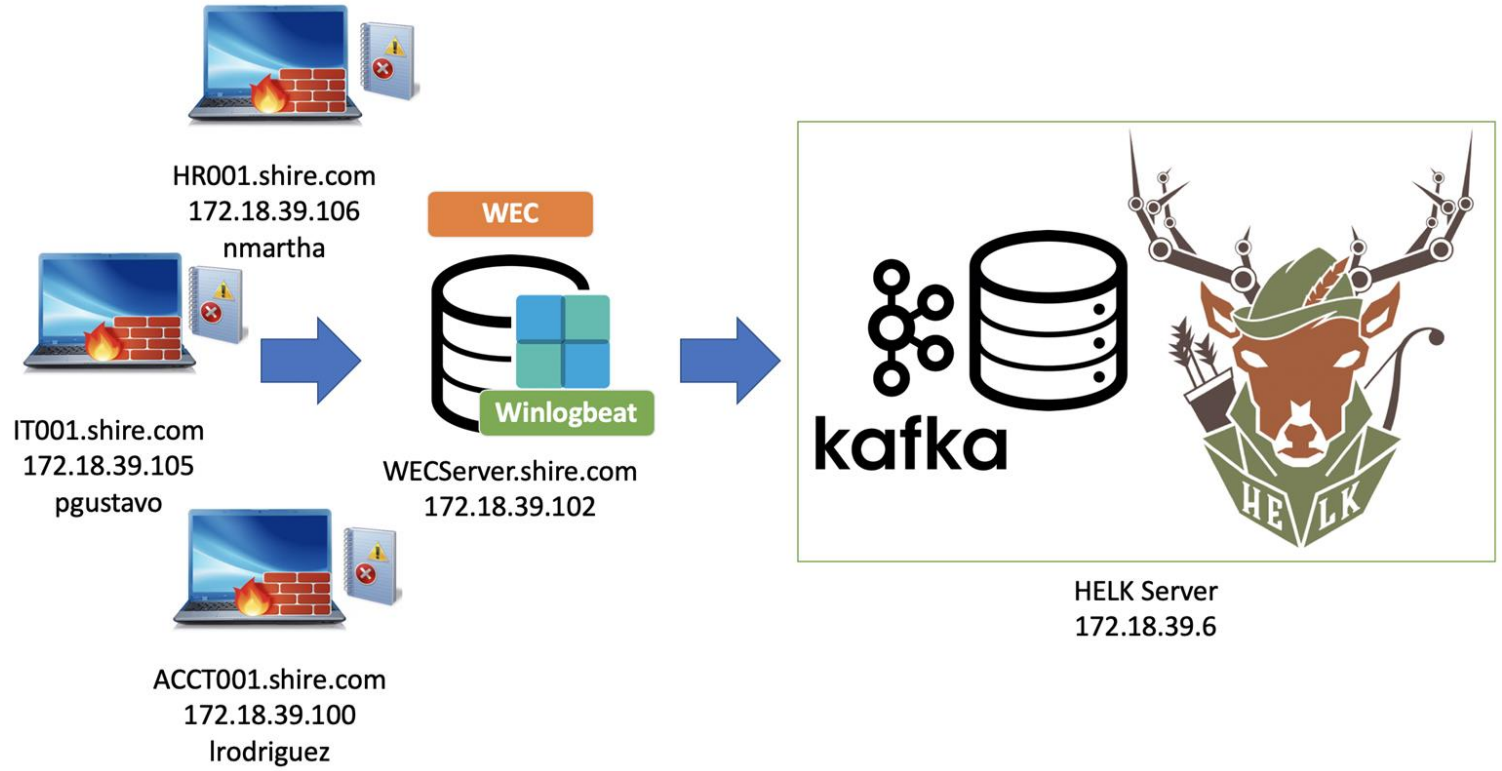


The Shire Telemetry: Win Logs & Sysmon



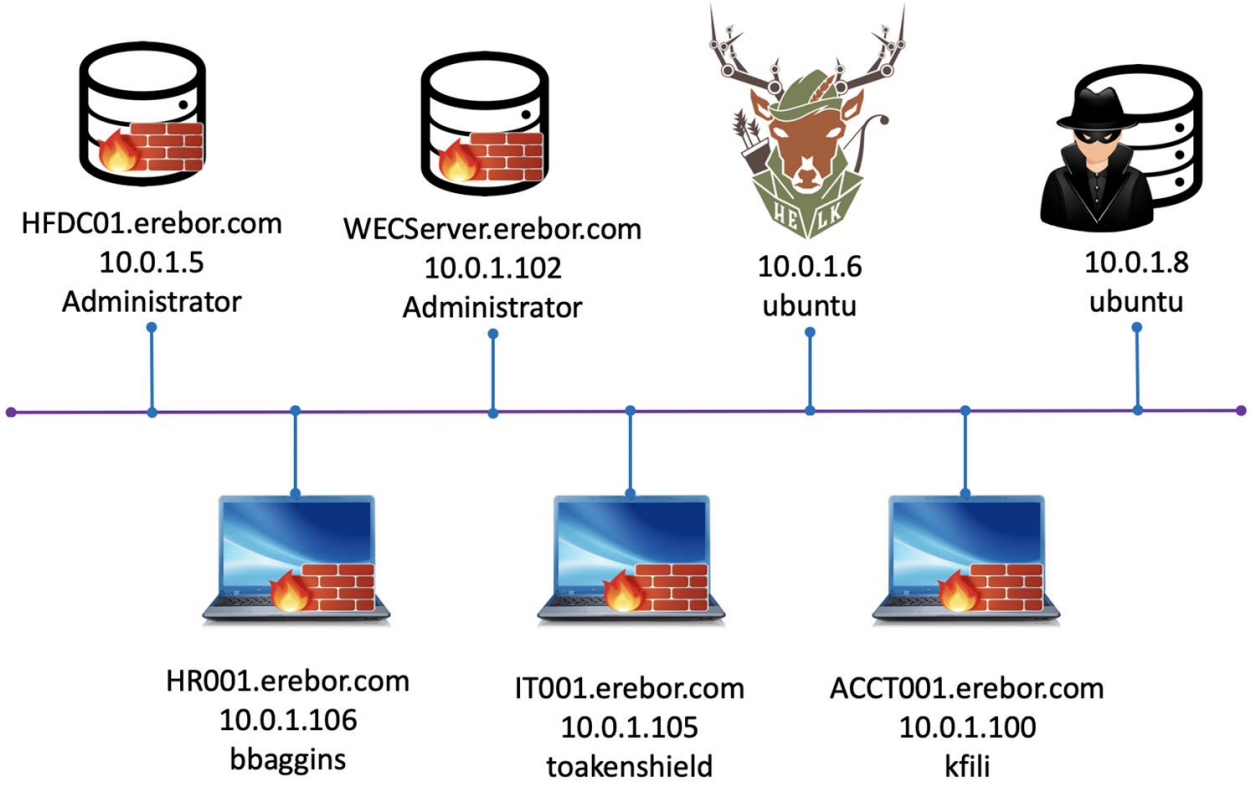
https://github.com/Cyb3rWard0g/OSSEM/tree/master/data_dictionaries/windows/sysmon

The Shire: Event Log -> WEC -> HELK

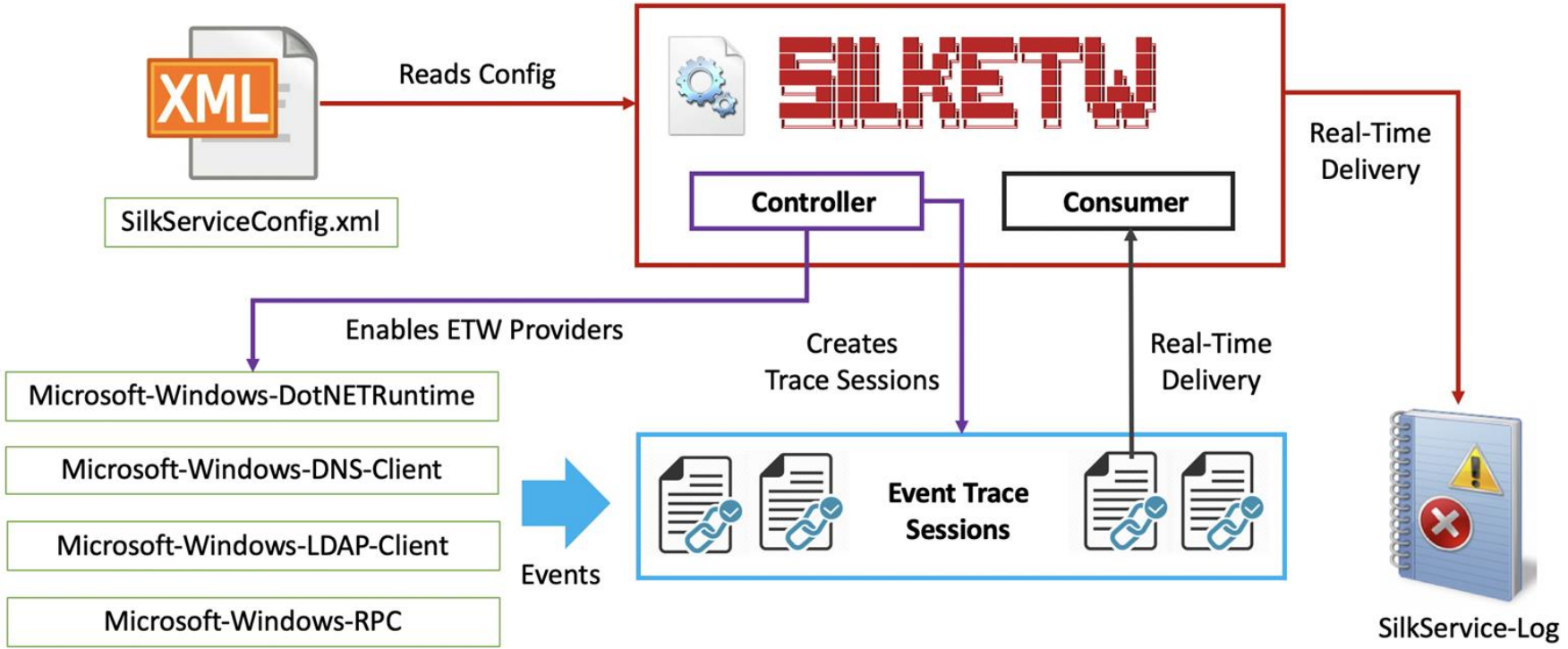


Mordor Environments: Erebor (Lonely Mountain)

Erebor Design

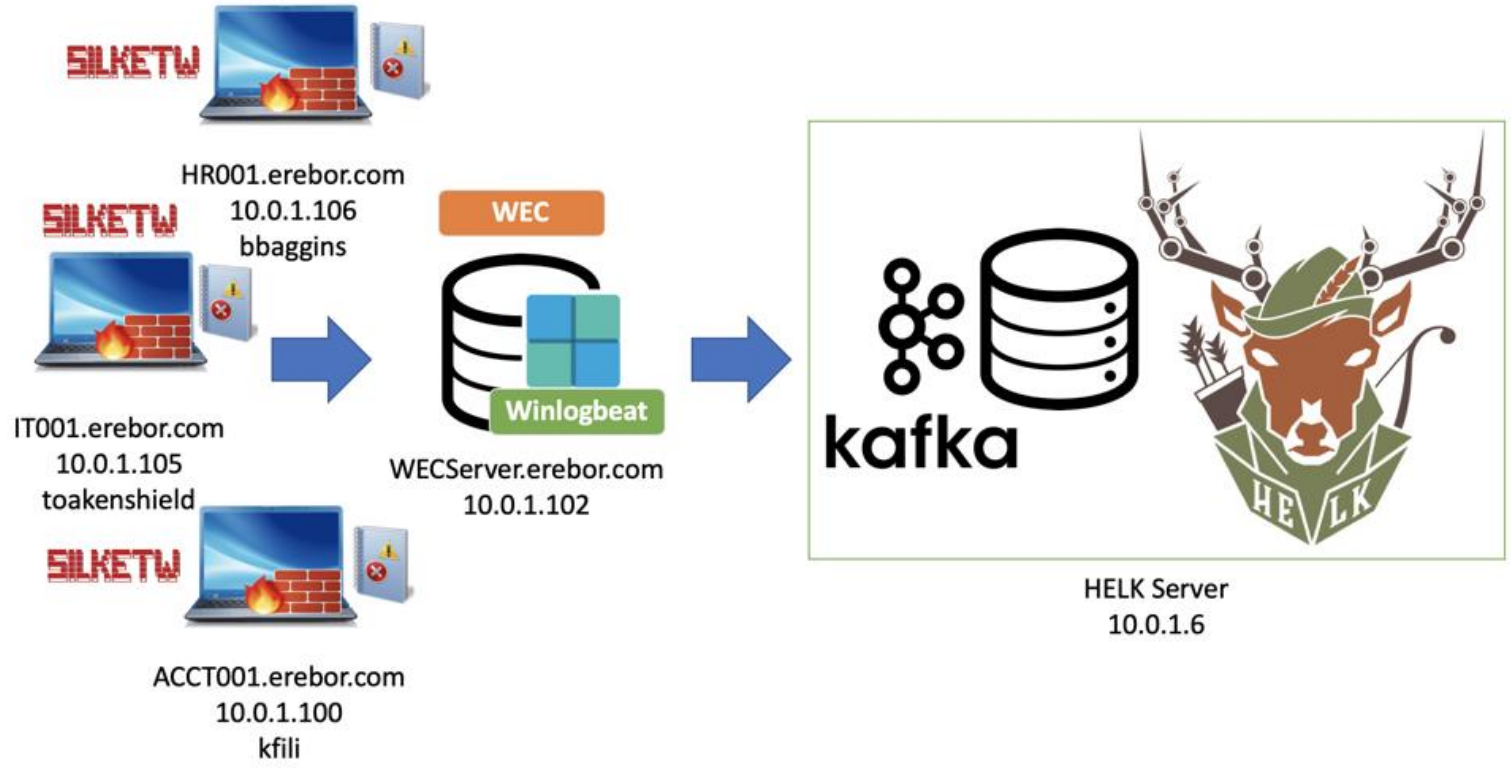


Erebor Telemetry: ETW Events via SilkETW



https://medium.com/threat-hunters-forge/threat-hunting-with-etw-events-and-helk-part-1-installing-silketw-6eb74815e4a0

Erebor: ETW Events -> Event Log -> WEC -> HELK



How do you collect data?

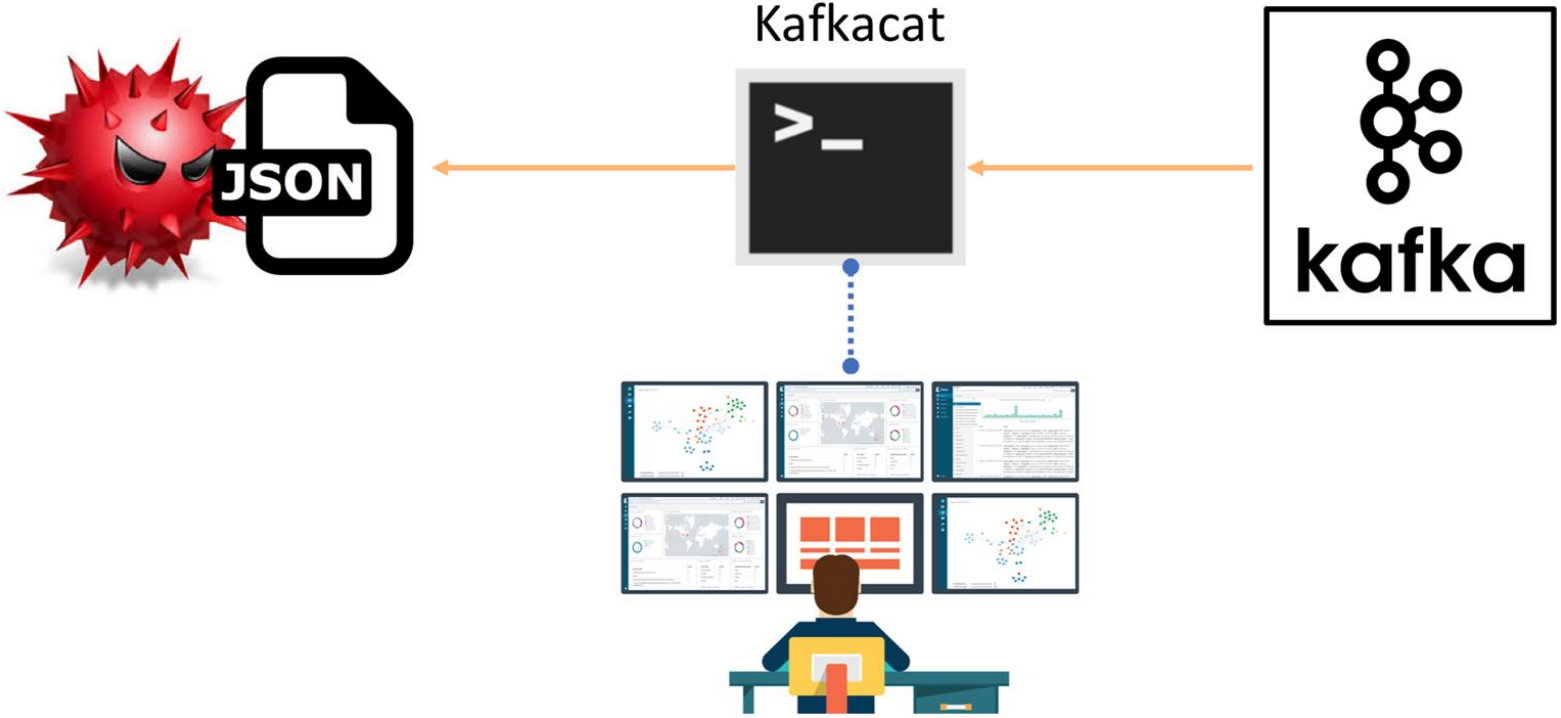
- We use **Kafkacat**!
- kafkacat is a generic non-JVM producer and consumer for Apache Kafka >=0.8, think of it as a netcat for Kafka.
- **In consumer mode**
  - Kafkacat reads messages from a topic and prints them to standard output (stdout). You can also redirect it to a file (i.e. JSON)
- **In producer mode**
  - Kafkacat reads messages from standard input (stdin). You can also send data to kafkacat by adding data from a file.

Consuming Data (Taking a snapshot of data)

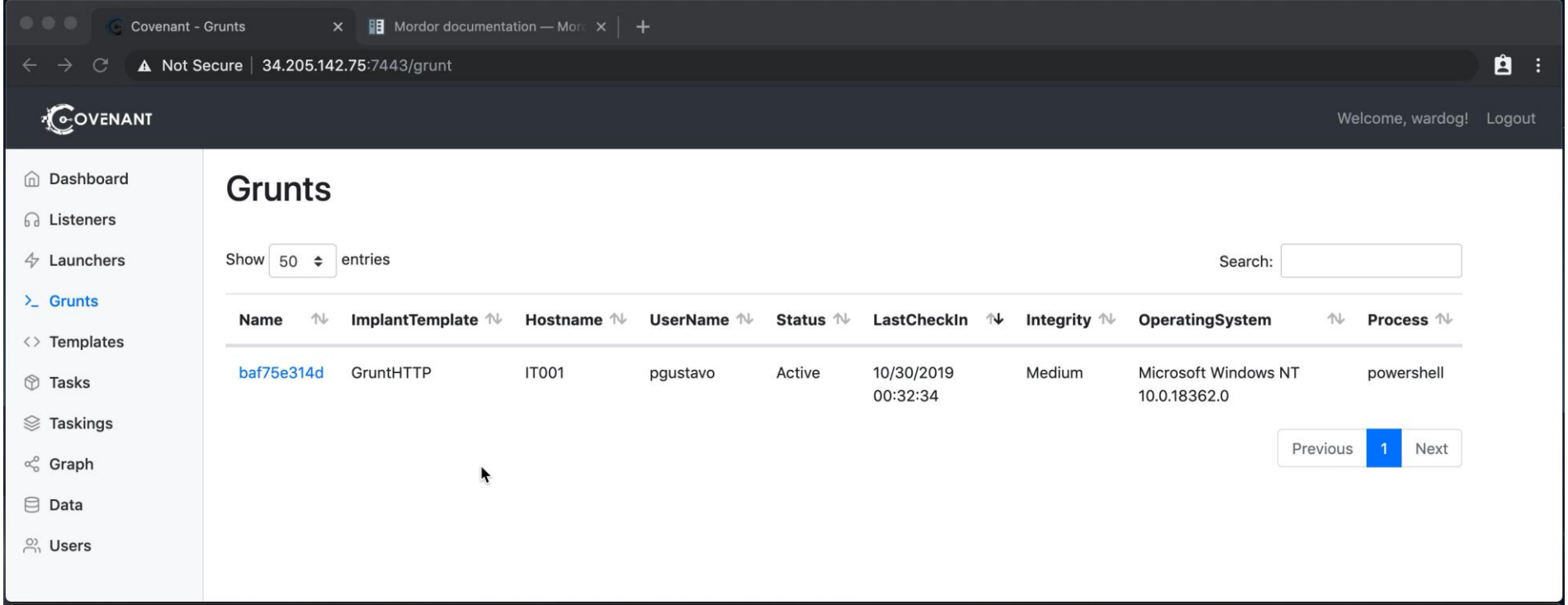
```
$ kafkacat -b <Kafka-IP>:9092 -t
<kafka-Topic> -C -o end > file.json
```

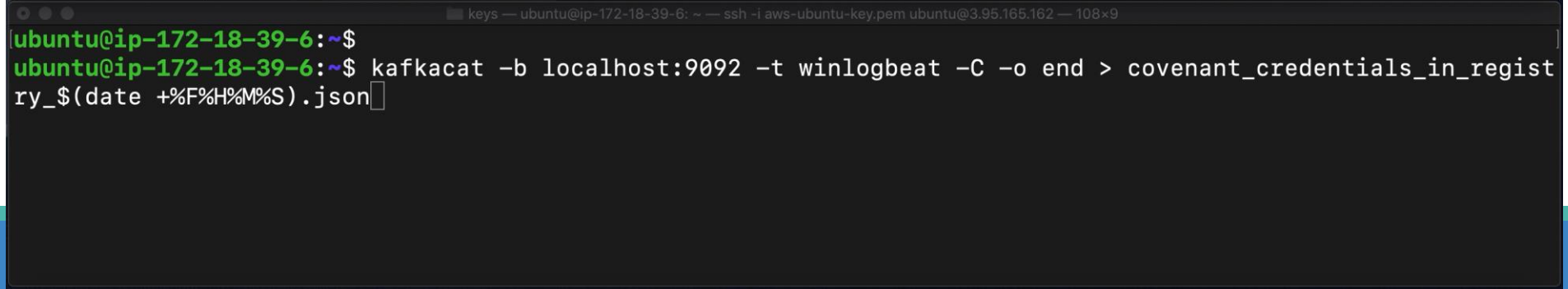
- **-b** : Kafka broker
- **-t** : Topic to consume from
- **-C** : Consumer Mode
- **-o** : Offset to start consuming from

Consuming Data -> Creating Mordor File (Video)

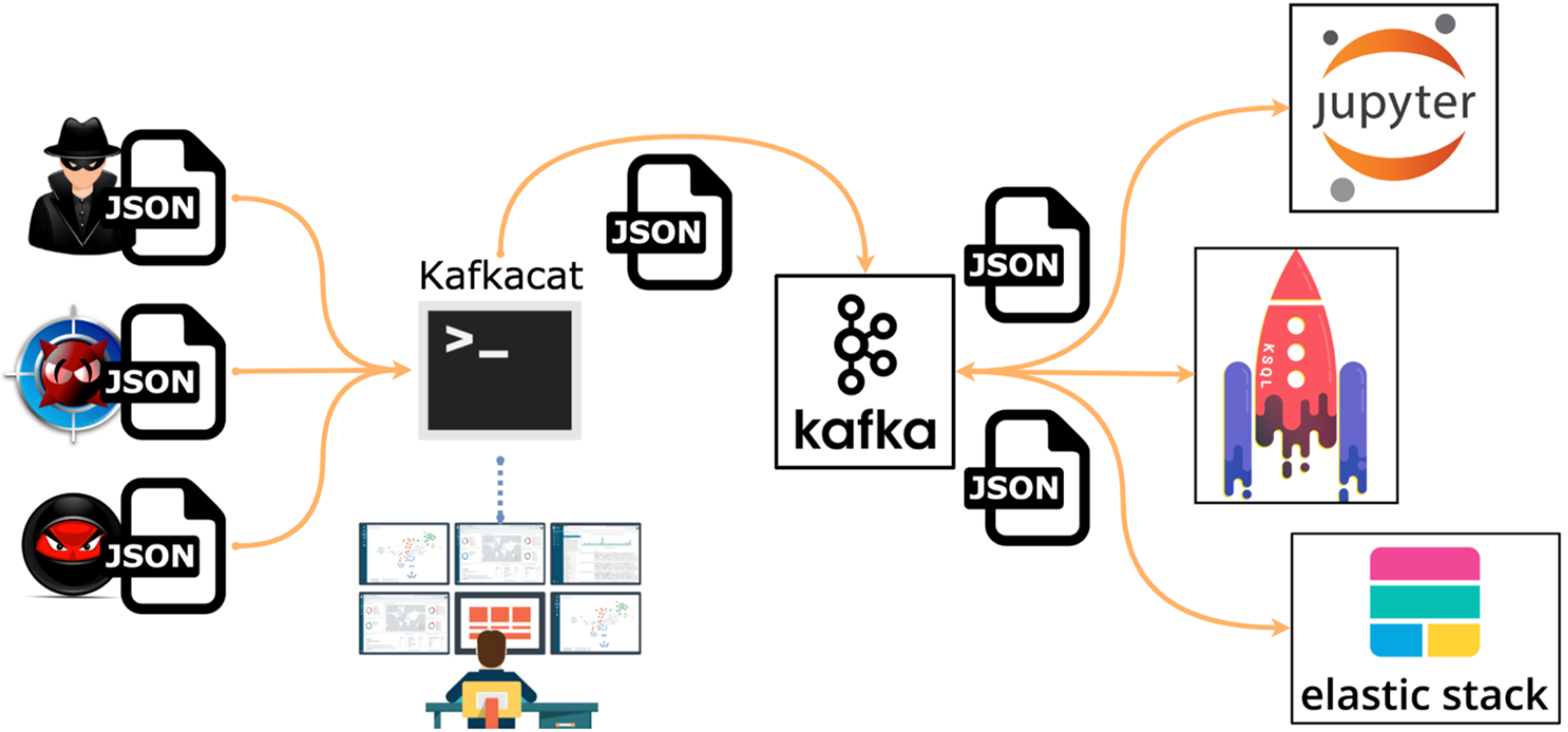


https://mordor.readthedocs.io/en/latest/export_mordor.html


Covenant - Grunts
Mordor documentation — Mor
Not Secure
34.205.142.75:7443/grunt
COVENANT
Welcome, wardog!
Logout
Dashboard
Listeners
Launchers
Grunts
Templates
Tasks
Taskings
Graph
Data
Users
Grunts
Show 50 entries
Search:
Name
ImplantTemplate
Hostname
UserName
Status
LastCheckIn
Integrity
OperatingSystem
Process
baf75e314d
GruntHTTP
IT001
pgustavo
Active
10/30/2019 00:32:34
Medium
Microsoft Windows NT 10.0.18362.0
powershell
Previous
1
Next


keys — ubuntu@ip-172-18-39-6: ~ — ssh -i aws-ubuntu-key.pem ubuntu@3.95.165.162 — 108×9
ubuntu@ip-172-18-39-6:~$
ubuntu@ip-172-18-39-6:~$ kafkacat -b localhost:9092 -t winlogbeat -C -o end > covenant_credentials_in_registry_$(date +%F%H%M%S).json

Producing Data (Injecting Adversary Dataset)



Producing Data (Injecting Adversary Dataset)

```
$ kafkacat -b <Kafka-IP>:9092 -t
<kafka-Topic> -P -l file.json
```

- **-b** : Kafka broker
- **-t** : Topic to produce to
- **-P** : Producer Mode
- **-l** : Send messages from a file

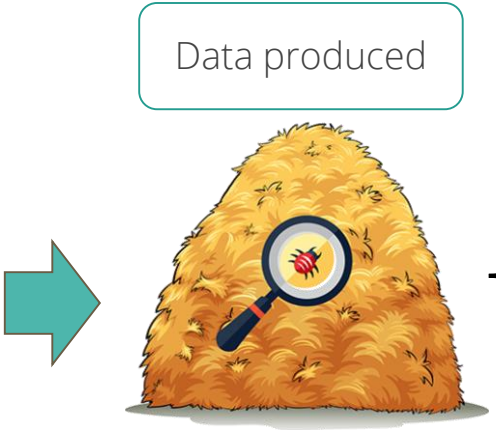
I just want to download all the datasets..

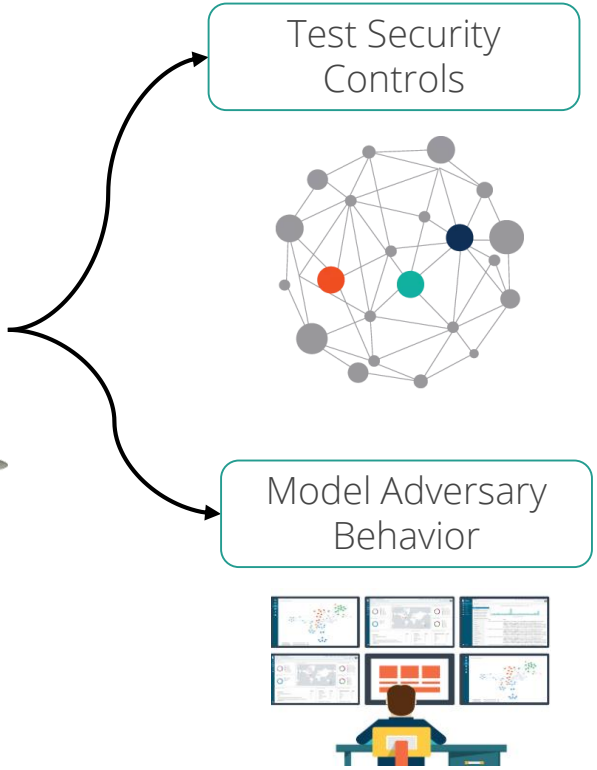
```
$ git clone https://github.com/hunters-forge/mordor.git
```

```
$ cd mordor/small_datasets/
```

```
$ find . -type f -name "*.tar.gz" -print0 | sudo xargs -0 -I{} tar xf {} -C .
```

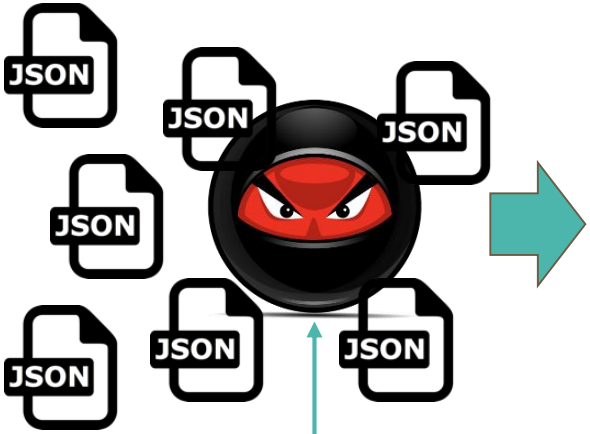
Expedite Analytics Validation!





YOU CAN DO IT NOW!

Validate Analytics!



Mordor File

Validate Analytics

2 + 2 = 4

Where do we get analytics from?

I have data with me and I am ready!

Mordor & CAR

The MITRE Cyber Analytics Repository (CAR)!

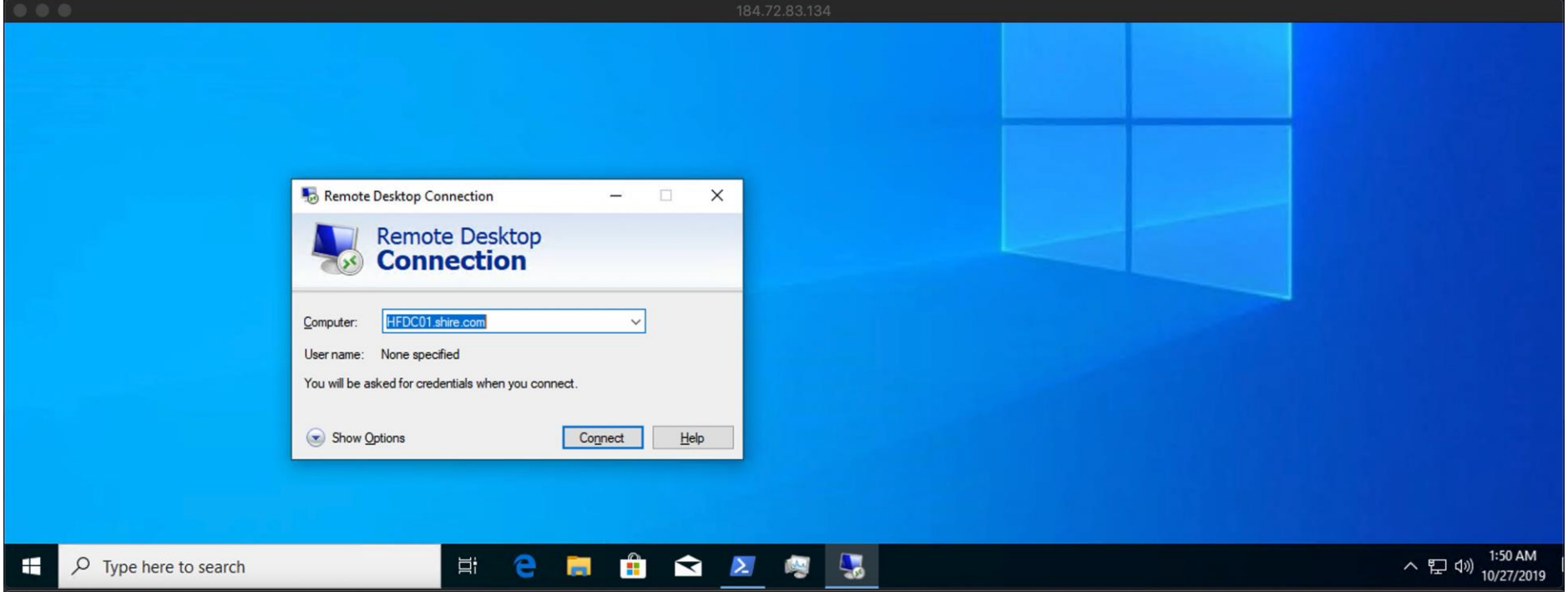
CAR-2019-08-001: Credential Dumping via Windows Task Manager

- The Windows Task Manager may be used to dump the memory space of lsass.exe to disk for processing with a credential access tool such as Mimikatz. This is performed by launching Task Manager as a privileged user, selecting lsass.exe, and clicking “Create dump file”. This saves a dump file to disk with a deterministic name that includes the name of the process being dumped.
- This requires filesystem data to determine whether files have been created.
- **Contributors:** Tony Lambert/Red Canary

But, How do I simulate that technique?

Interactive Task Manager Lsass dump (Demo 03)

https://github.com/hunters-forge/mordor/blob/master/small_datasets/windows/credential_access/credential_dumping_T1003/interactive_taskmngr_lsass_dump.md



mordor_extras — ubuntu@ip-172-18-39-6: ~ — ssh -i ../projects/keys/aws-ubuntu-key.pem ubuntu@3.83.254.137 — 116×10

```
ubuntu@ip-172-18-39-6:~$
ubuntu@ip-172-18-39-6:~$ kafkacat -b localhost:9092 -t winlogbeat -C -o end > remoteinteractive_taskmngr_lsass_dump_
$(date +%F%H%M%S).json
```

CAR-2019-08-001: Procdump - File Create (Pseudocode)

```
files = search File:Create

lsass_dump = filter files where (

  file_name = "lsass*.dmp"  and

  image_path = "C:\Windows\*\taskmgr.exe")

output lsass_dump
```

But, where do I run that?

Enter Jupyter Notebooks

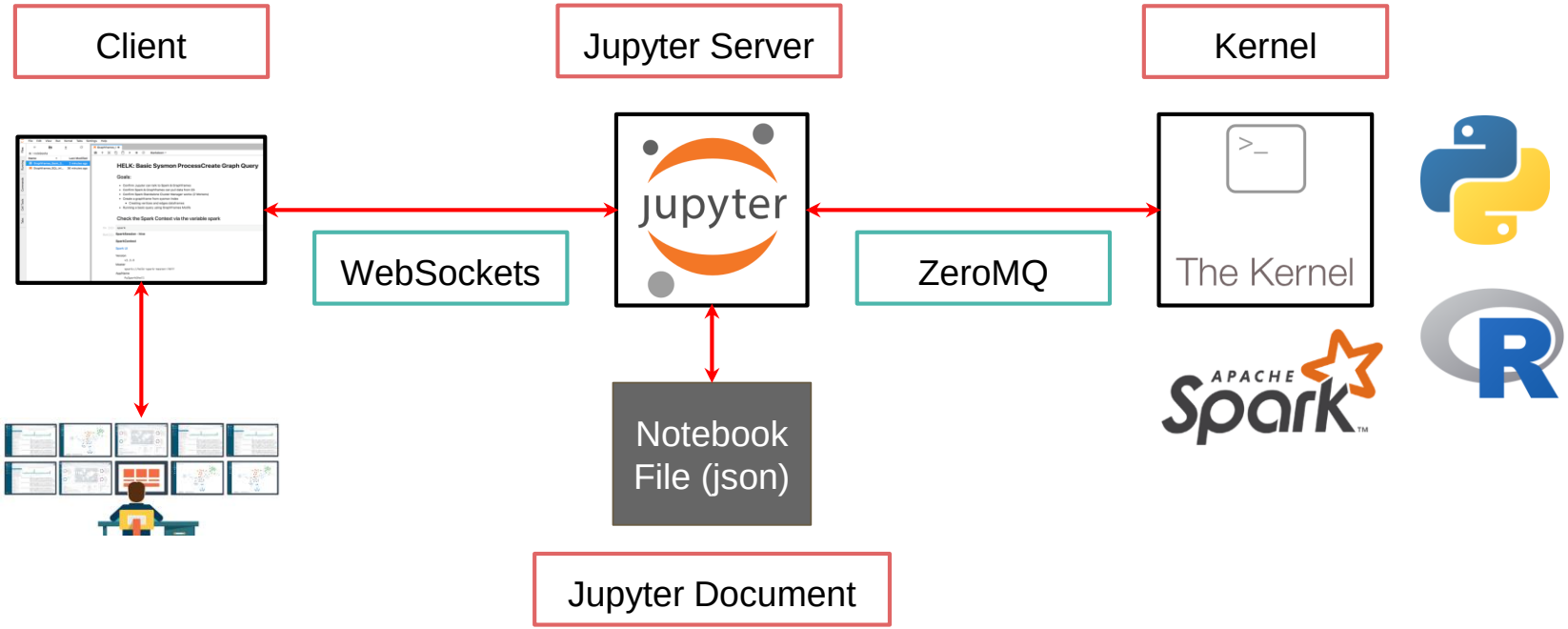
What are Jupyter Notebooks?

- Think of a notebook as a document that you can access via a web interface that allows you to save:
  - **Input** (live code)
  - **Output** (evaluated code output)
  - **Visualizations and narrative text** (Tell the story!)
- Uses include:
  - Data cleaning and transformation
  - Statistical modeling
  - Data visualization
  - Machine learning, and much more

How Do Jupyter Notebooks Work?

- Jupyter Notebooks work with what is called a **two-process model** based on a **kernel-client** infrastructure.
- This model applies **Read-Evaluate-Print Loop (REPL)**:
  - Takes a single user's inputs
  - Evaluates them
  - Returns the result to the user

Jupyter Notebooks Architecture



Mordor -> Jupyter Notebooks

CAR-2019-08-001: Credential Dumping via Windows Task Manager

The ThreatHunter-Playbook @HunterPlaybook

- A Threat hunter's playbook to aid the development of techniques and hypothesis for hunting campaigns by leveraging security event logs from diverse operating systems.
- It documents detection strategies in the form of **interactive notebooks** to provide an easy and flexible way to visualize the expected output and be able to **run the analytics against pre-recorded mordor datasets**

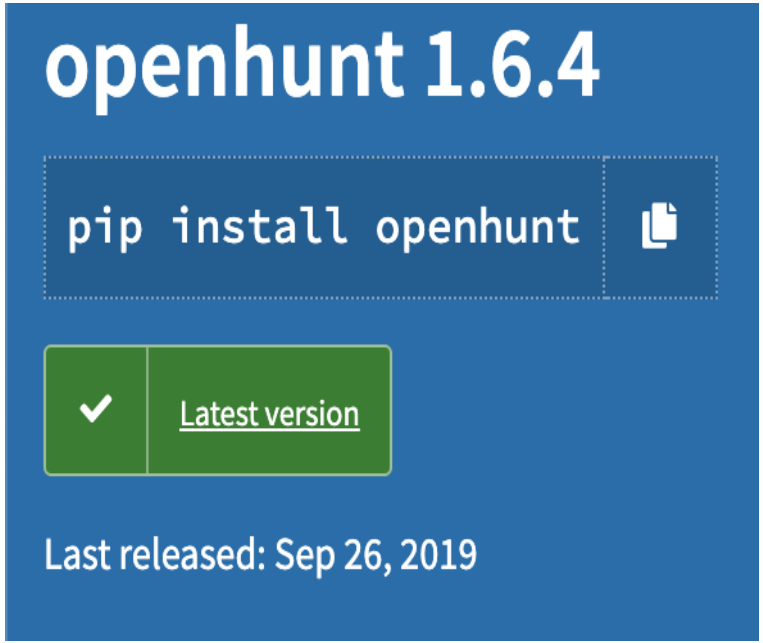
OpenHunt Library

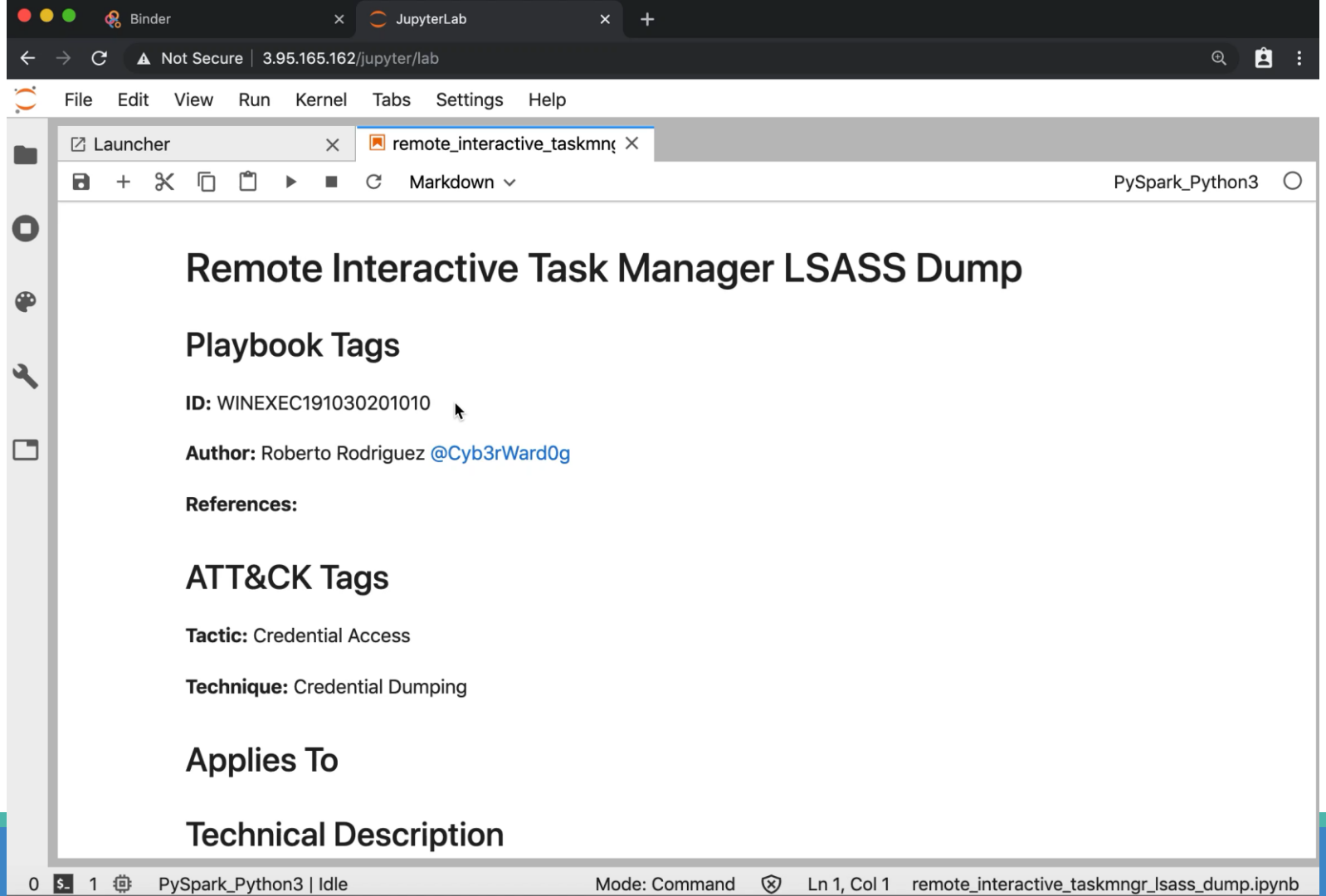
- **Via PIP:**

```
pip install openhunt
```

- **Or Straight from Source**

```
git clone
https://github.com/Cyb3rPanda/openhunt

cd OpenHunt && pip install .
```

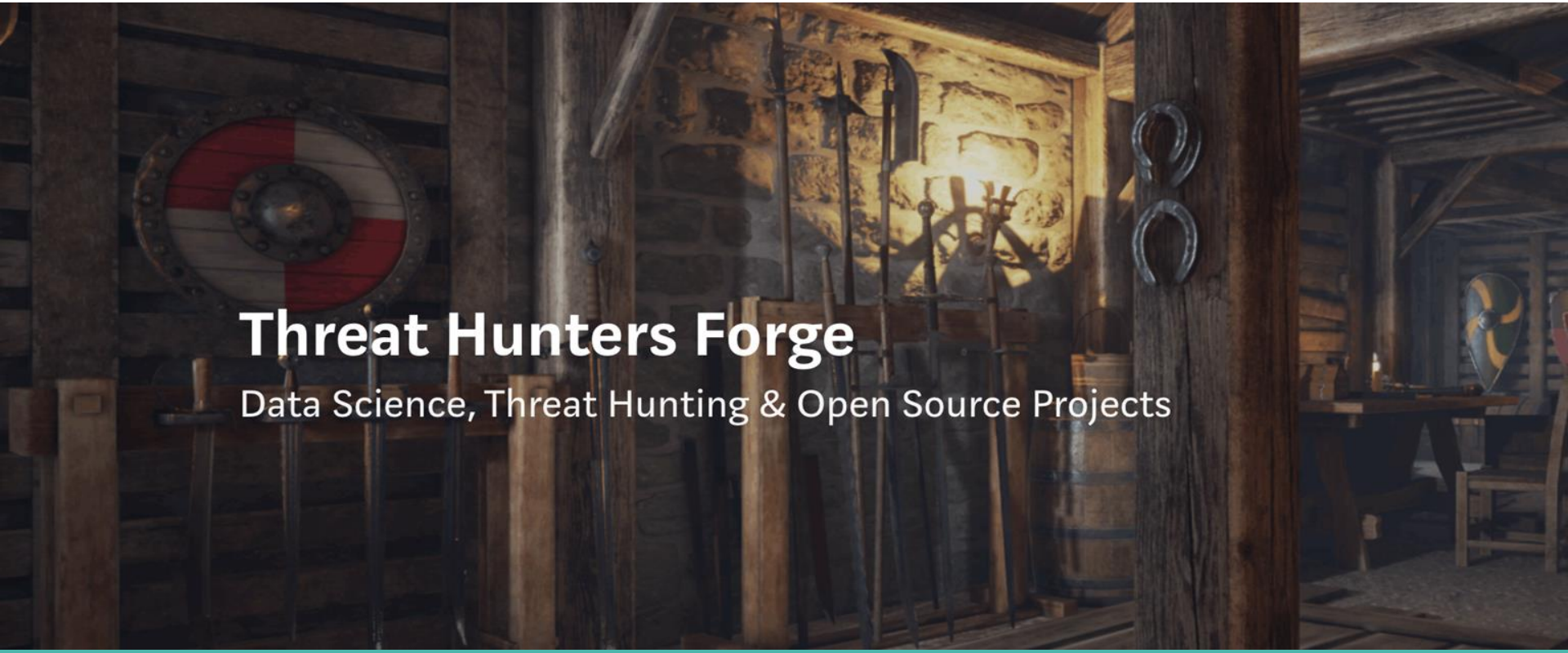



Binder
JupyterLab
Not Secure | 3.95.165.162/jupyter/lab
File Edit View Run Kernel Tabs Settings Help
Launcher
remote_interactive_taskmng
Markdown
PySpark_Python3
Remote Interactive Task Manager LSASS Dump
Playbook Tags
ID: WINEXEC191030201010
Author: Roberto Rodriguez @Cyb3rWard0g
References:
ATT&CK Tags
Tactic: Credential Access
Technique: Credential Dumping
Applies To
Technical Description
0 1 PySpark_Python3 | Idle
Mode: Command
Ln 1, Col 1
remote_interactive_taskmngr_lsass_dump.ipynb

Is You Ready? haha

Hunt The Planet!

Threat Hunters Forge Community!



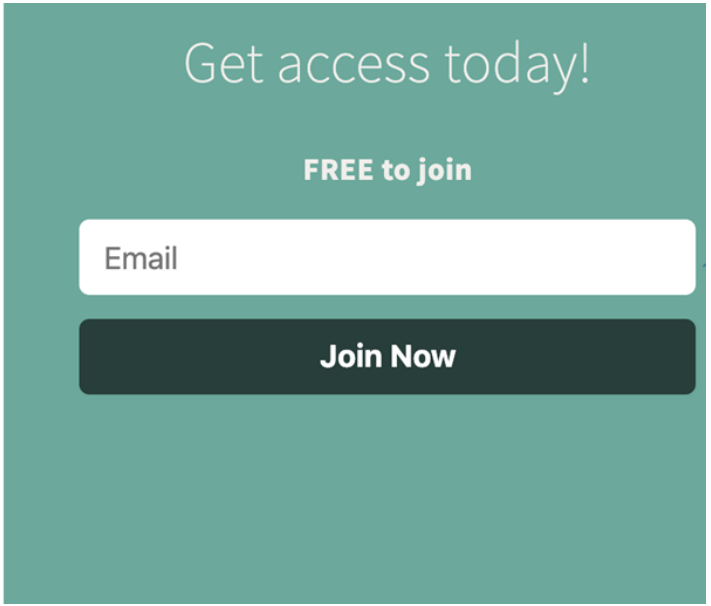
Threat Hunters Forge Slack Community!

ThreatHunting

Threat Hunters Forge

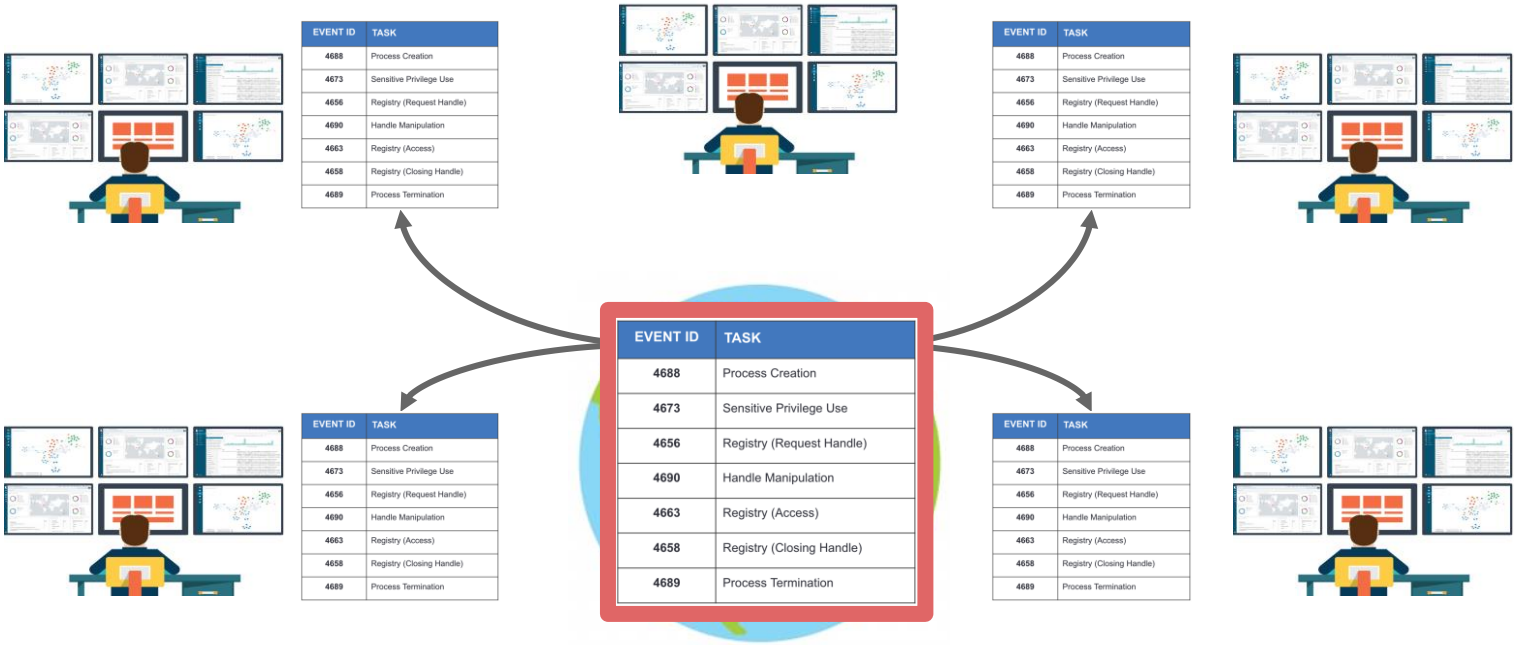
Join the Threat Hunters Forge Slack Community!

A community led effort to share detection strategies and to support open source projects to aid the development of security analytics and tooling for threat hunting!

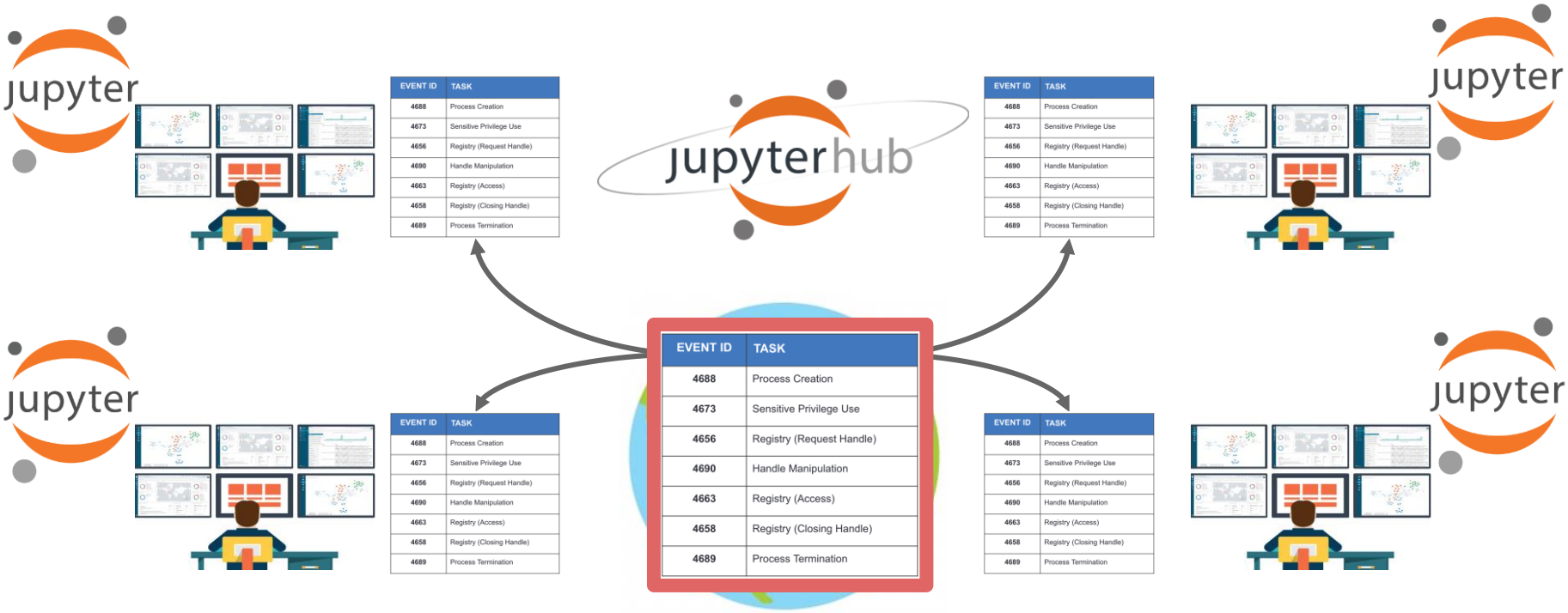


https://launchpass.com/threathunting

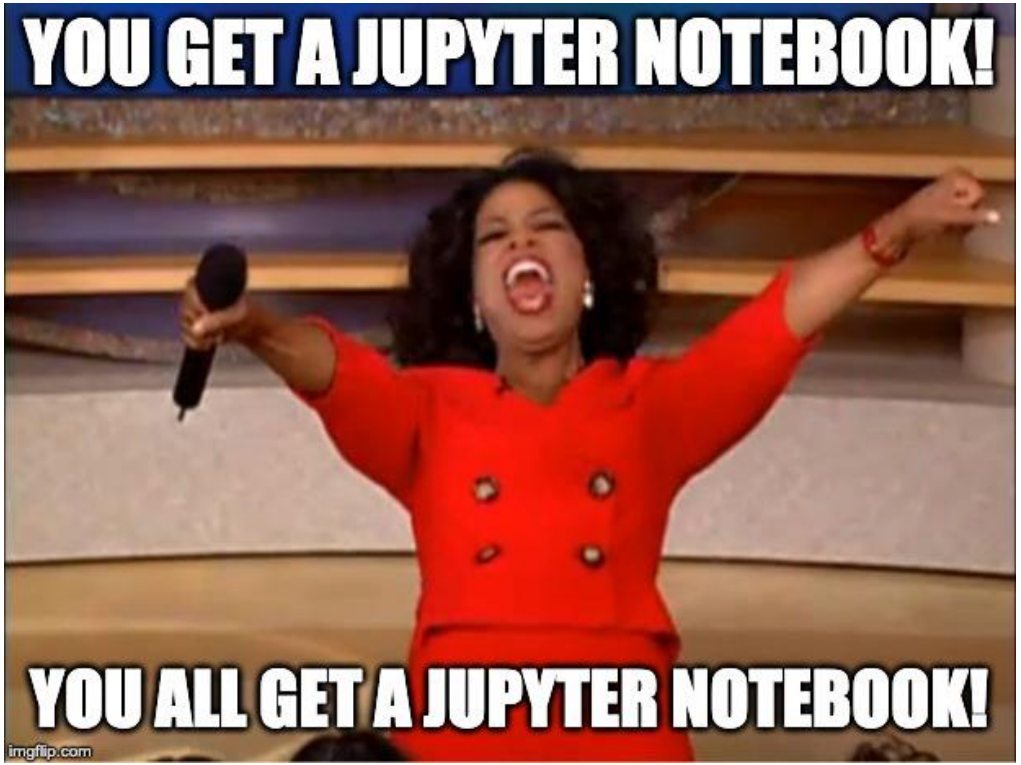
Remember this initiative with Mordor?



What if everyone gets a notebook too?



Wait, Whaaat?


YOU GET A JUPYTER NOTEBOOK!
YOU ALL GET A JUPYTER NOTEBOOK!
imgflip.com

Wait, Whaaat?

The Binder Project

- The Binder Project is an open community that makes it possible to create shareable, interactive, reproducible environments.
- The main technical product that the community creates is called **BinderHub**, and one deployment of a BinderHub exists at **mybinder.org**.
- Who is it for?:
  - **Researchers**, **Educators**, **people analyzing data** and **people trying to communicate the data analysis to others**!!

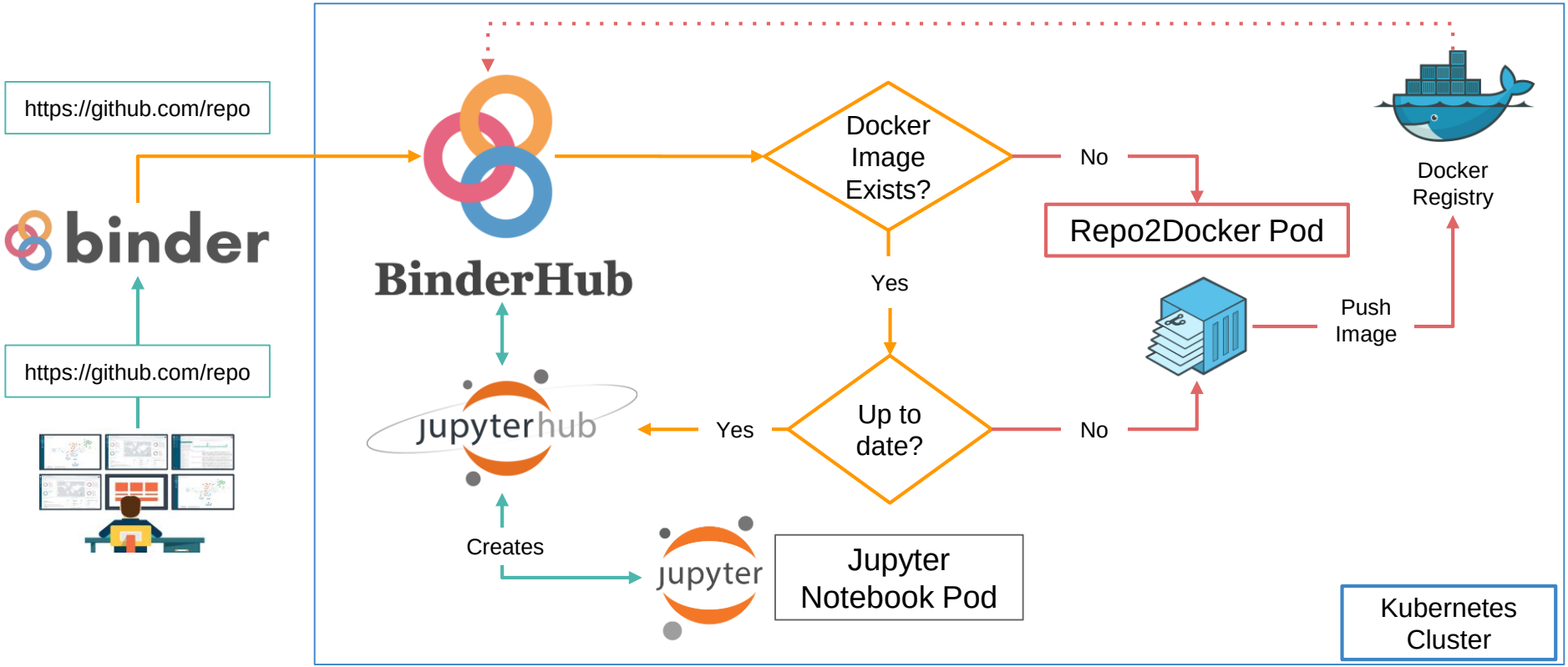
https://mybinder.readthedocs.io/en/latest/introduction.html#what-is-the-binder-project

BinderHub

BinderHub connects several services together to provide on-the-fly creation and registry of Docker images. It utilizes the following tools:

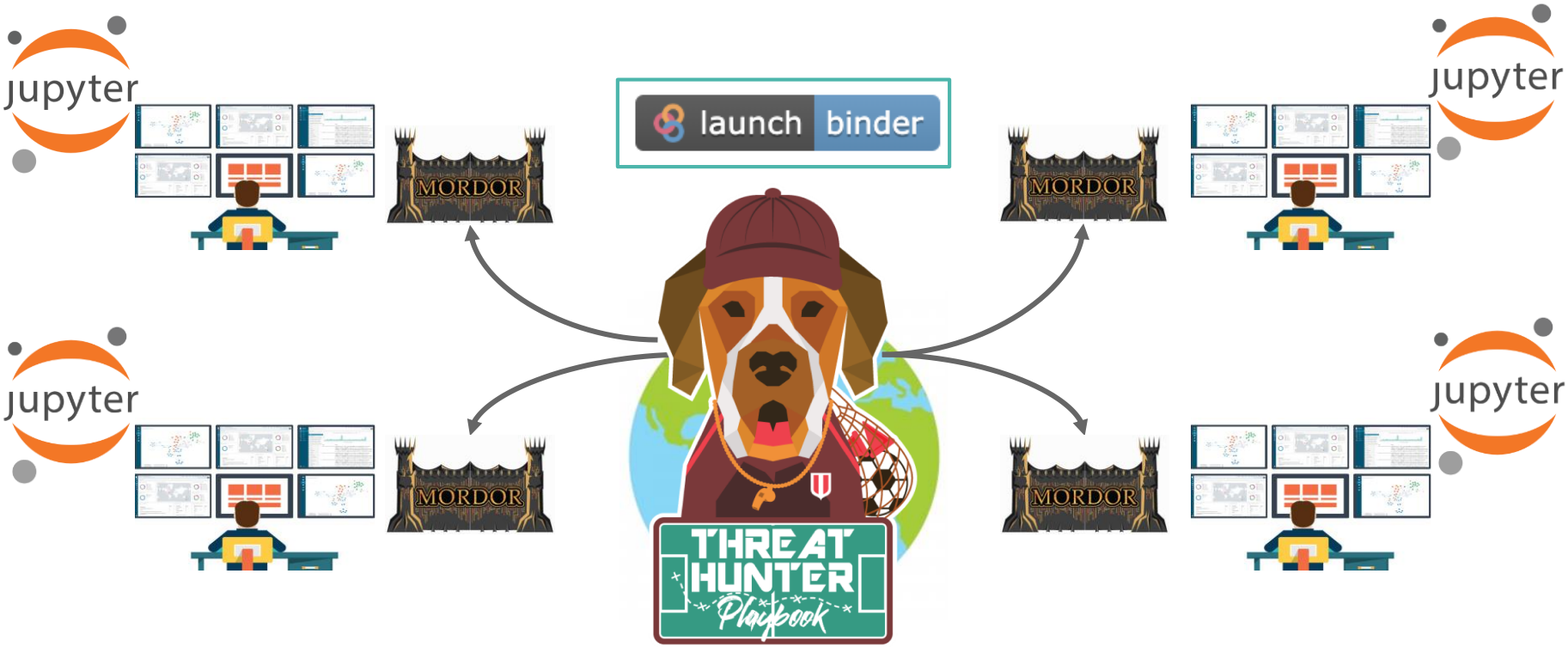
- **A cloud provider** such Google Cloud, Microsoft Azure, Amazon EC2, and others
- **Kubernetes** to manage resources on the cloud
- **Helm** to configure and control Kubernetes
- **Docker** to use containers that standardize computing environments
- **A BinderHub UI** that users can access to specify Git repos they want built
- **BinderHub** to generate Docker images using the URL of a Git repository
- **A Docker registry** (such as gcr.io) that hosts container images
- **JupyterHub** to deploy temporary containers for users

Binder Design!



https://binderhub.readthedocs.io/en/latest/overview.html#a-diagram-of-the-binderhub-architecture

Open Infrastructure for Open Hunts!

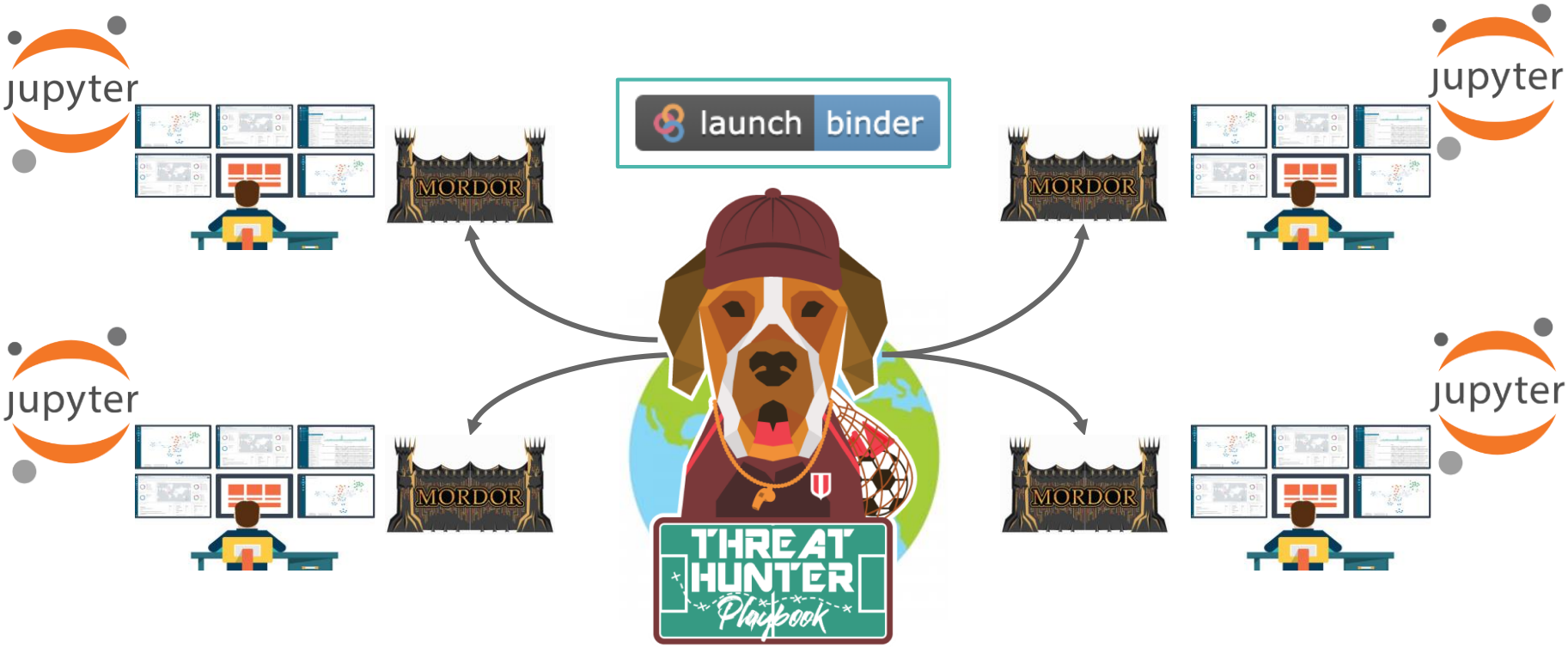


https://github.com/hunters-forge/ThreatHunter-Playbook

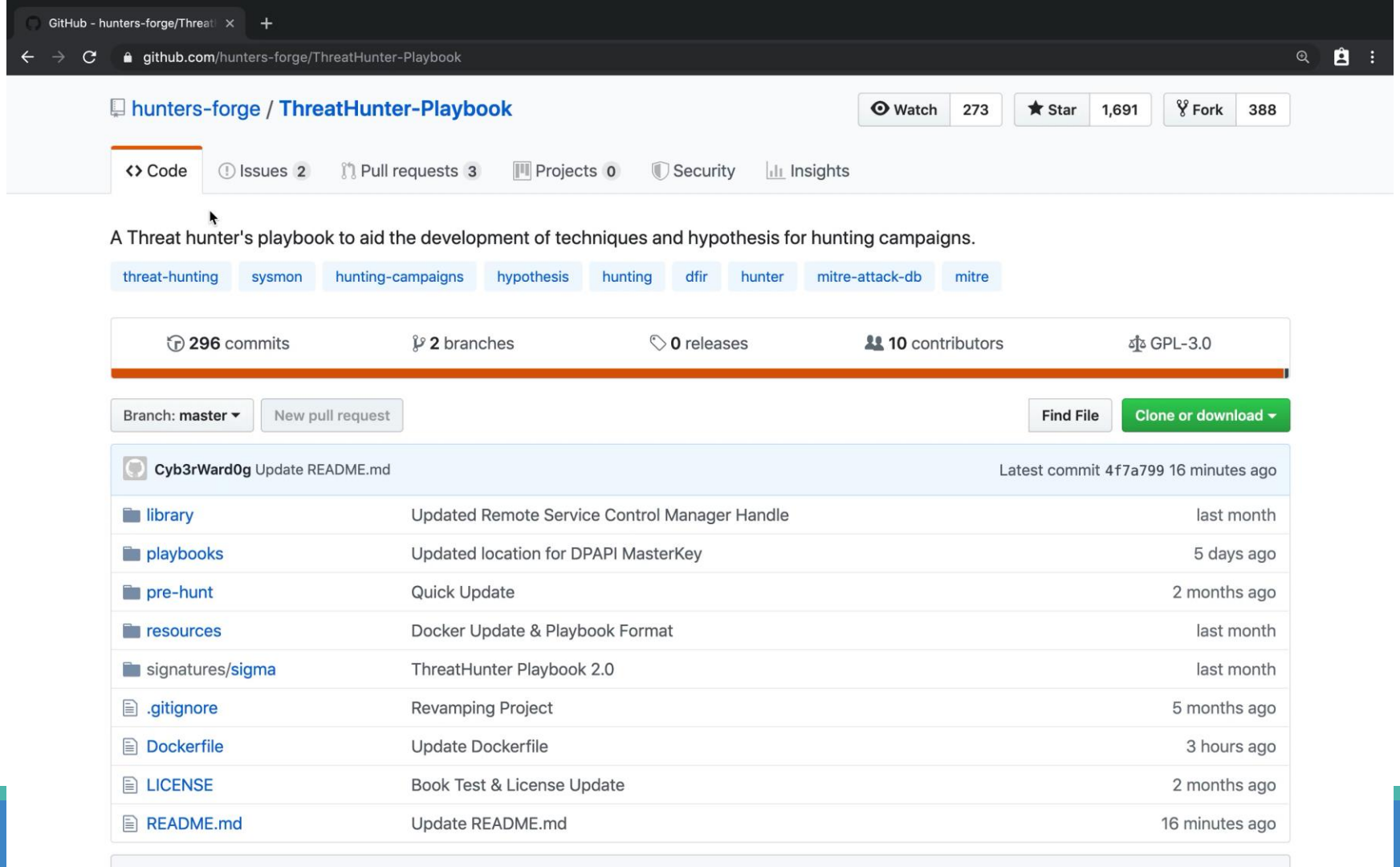
Open Infrastructure for Open Hunts! (LIVE!)

```
https://mybinder.org/v2/gh/hunters-forge/ThreatHunter-Playbook/master
```

Threat Hunter Playbooks via Binder (Video)



https://github.com/hunters-forge/ThreatHunter-Playbook


GitHub - hunters-forge/Threat
github.com/hunters-forge/ThreatHunter-Playbook
hunters-forge / ThreatHunter-Playbook
Watch 273
Star 1,691
Fork 388
Code
Issues 2
Pull requests 3
Projects 0
Security
Insights
A Threat hunter's playbook to aid the development of techniques and hypothesis for hunting campaigns.
threat-hunting
sysmon
hunting-campaigns
hypothesis
hunting
dfir
hunter
mitre-attack-db
mitre
296 commits
2 branches
0 releases
10 contributors
GPL-3.0
Branch: master
New pull request
Find File
Clone or download
Cyb3rWard0g Update README.md
Latest commit 4f7a799 16 minutes ago
library
Updated Remote Service Control Manager Handle
last month
playbooks
Updated location for DPAPI MasterKey
5 days ago
pre-hunt
Quick Update
2 months ago
resources
Docker Update & Playbook Format
last month
signatures/sigma
ThreatHunter Playbook 2.0
last month
.gitignore
Revamping Project
5 months ago
Dockerfile
Update Dockerfile
3 hours ago
LICENSE
Book Test & License Update
2 months ago
README.md
Update README.md
16 minutes ago

Goal: Share and Empower the Community!

Let’s do it together!

Threat Hunters Forge References

- **GitHub**: https://github.com/hunters-forge
- **Python Library**: https://github.com/Cyb3rPanda/openhunt
- **Slack Invitation**: https://launchpass.com/threathunting
- **Official Blog**: https://medium.com/threat-hunters-forge
- **Founders**: @Cyb3rWard0g & @Cyb3rPandaH
- **Official Twitter:** @HuntersForge
- @HunterPlaybook
- @THE_HELK
- @OSSEM_Project, @Mordor_Project & More

Thank You! Muchas Gracias!