

*WHEN WORLDS COLLIDE*

# OSS HUNTING AND ADVERSARIAL SIMULATION

*WITH BHIS & FRIENDS*

**BLACK HILLS** | Information Security

WEBCAST

# OSS Hunting and Adversarial Simulation

What are we doing here?



Pre-Show Banter



Panelist Discussion: OSS Community Problems



Project Spotlight: Open Threat Research

# Hosts and Panel



## Hosts:

- Jordan Drysdale
- Kent Ickler

- @rev10d
- @krelkci

- Security Analysts, OSS Contributors, Instructors
- Black Hills Information Security
- Defensive Origins



**Roberto Rodriguez**

- @Cyb3rWard0g
- Microsoft Threat Intelligence Center
- OSS Developer



**Nate Guagenti**

- @neu5ron
- SOCPrime
- OSS Developer



**Marcello Salvati**

- @byt3bl33d3r
- Black Hills InfoSec
- Security Analyst
- OSS Developer



**John Strand**

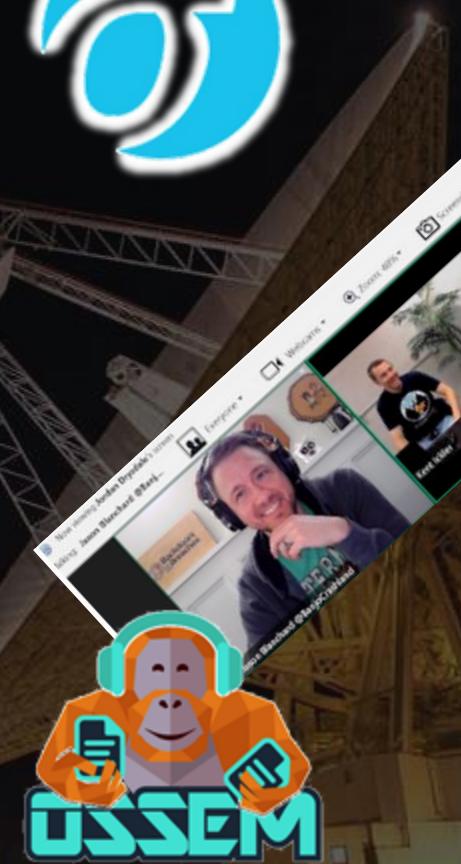
- @strandjs
- Black Hills InfoSec
- Thought Leader, Instructor

# What Brought Us Here? Red v Blue Dichotomy?

Actually no. Open Source(ry) Networking. And late nights



SILENTTRINITY



# Executive Problem Statement



## OSS Community ^ Discussion

### Threat Intelligence Sharing

Lots of orgs still fail at basic threat optics

- Is it getting better?
  - Yes! Definitely, purple teams are growing (and sharing)

### Hackers Won't Stop

- Is defenders f
- Is it getting
  - Yes, s
  - Adver

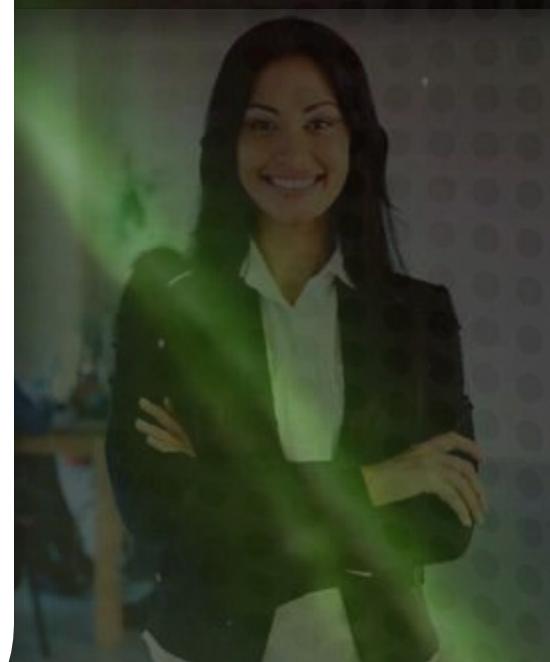
### (Non-Monetized)

- Late night
- Duplicated
- Is it gettin

### Re-Investing O

- WWHF Tr
- Commerci

A screenshot of a Google Slides presentation titled "Why I Hate Threat Intel". The slide features a dark background with several images: a collection of colorful mushrooms, a shark breaching the water, a pufferfish, a bear, and a group of cavemen. The presentation has a sidebar with thumbnails of other slides. At the bottom, there is a logo for "BLACK HILLS INFORMATION SECURITY" and a copyright notice. The video player interface shows the video is at 4:07 / 1:15:05.



# Executive Problem Statement

## OSS Community ^ Discussion



### Threat Intelligence Sharing

Lots of orgs still fail at basic threat optics

- Is it getting better?
  - Yes! Definitely, purple teams are growing (and sharing)

### Hackers Won't Stop

- Is defenders fatigue a thing?
- Is it getting better?
  - Yes, see: Elastic, Sysmon, MS Defender, ATP
  - Adversarial Simulation (ART / Mordor)

Open Source Community is Tired

Marcello (@pytobuzz) · Sep 1  
Got AppDomainManager injection working remotely last night, this download the assembly over HTTP (!) or a UNC path. As a bonus, also disables ETW thanks to the built in etwEnable runtime configuration option.

( GitHub Gist · Remote AppDomainManager Injection · GitHub Gist: instantly share code notes, and snippets. · gist.github.com )

Roberto Rodriguez Retweeted

Mordor (@Mordor\_Project) · 19h  
Ever wonder what you can do with our pre-recorded datasets? Take a look at how the @HunterPlaybook project uses them to share a few detection ideas through @ProjectJupyter notebooks with the InfoSec community 🌎  
@OTR\_Community

ThreatHunter-Playbook (@HunterPlaybook) · 19h  
"Adversaries might be leveraging WMI event subscriptions (ActiveScriptEventConsumers) for remote code execution" @OTR\_Community 🌎

Playbook: threathunterplaybook.com/notebooks/wind...

@Mordor\_Project datasets: mordordatasets.com/notebooks/sm...

Reference: @domchell mdsec.co.uk/2020/09/i-like...

strandjs @strandjs · 18h  
Malware of the day!!!! Comfoo!

**Malware of the Day**

Malware of the Day - Comfoo - Active Countermeasures  
What is Malware of the Day? Malware of the Day: COMFOO Lab Setup  
Malware: Comfoo AKA: Comfoo RAT Traffic Type: APT [...] activecountermeasures.com

1 7 11

Your One Rule.

Don't get caught..  
Don't get caught..  
Don't get caught..  
Don't get caught..  
Don't get caught..

TONIGHT  
YOU'RE GONNA BREAK  
YOUR ONE RULE

# Executive Problem Statement



## OSS Community ^ Discussion

### Threat Intelligence Sharing

Lots of orgs still sharing threat intel

- Is it growing?

### Hackers

- Is it growing?
- Is it more advanced?
- Is it more sophisticated?
- Is it more coordinated?
- Is it more effective? (e.g., Sysmon, MS Defender, ATP)
- Adversarial Simulation (ART / Mordor)



### (Non-Monetized) Open Source Community is Tired...

- Late nights coding
- Duplicated efforts, even small teams.
- Is it getting better?



### Re-Investing Open Source Projects

- WWHF Training Investment Approach
- Commercial Organizations



# Executive Problem Statement



## OSS Community ^ Discussion

### Threat Intelligence Sharing

Lots of orgs still fail at basic threat optics

- Is it getting better?
  - Yes! Definitely, purple teams are growing (and sharing)

### Hackers Won't Stop

- Is defenders fatigue a thing?
- Is it getting better?
  - Yes, see: Elastic, SANS, etc.
  - Adversarial Simulation

### (Non-Monetized) Open Source

- Late nights coding
- Duplicated efforts, even small teams.
- Is it getting better?

### Re-Investing Open Source Projects

- WWHF Training Investment Approach
- Commercial Organizations

strandjs @strandjs · Aug 6  
At [@WWHackinFest](#) we ran a management class with [@Chris\\_Brenton](#). The 10% (\$2,172.50) of that class is going to [@securityonion](#). Lets all thank [@dougburks](#) and team for all they do for the community!  
[wildwesthackinfest.com/deadwood/train...](http://wildwesthackinfest.com/deadwood/train...)

2 10 59



## OSS Community ^ Discussion



### Audience Questions



# OSS Hunting and Adversarial Simulation

What are we doing here?



Pre-Show Banter



Panelist Discussion: OSS Community Problems



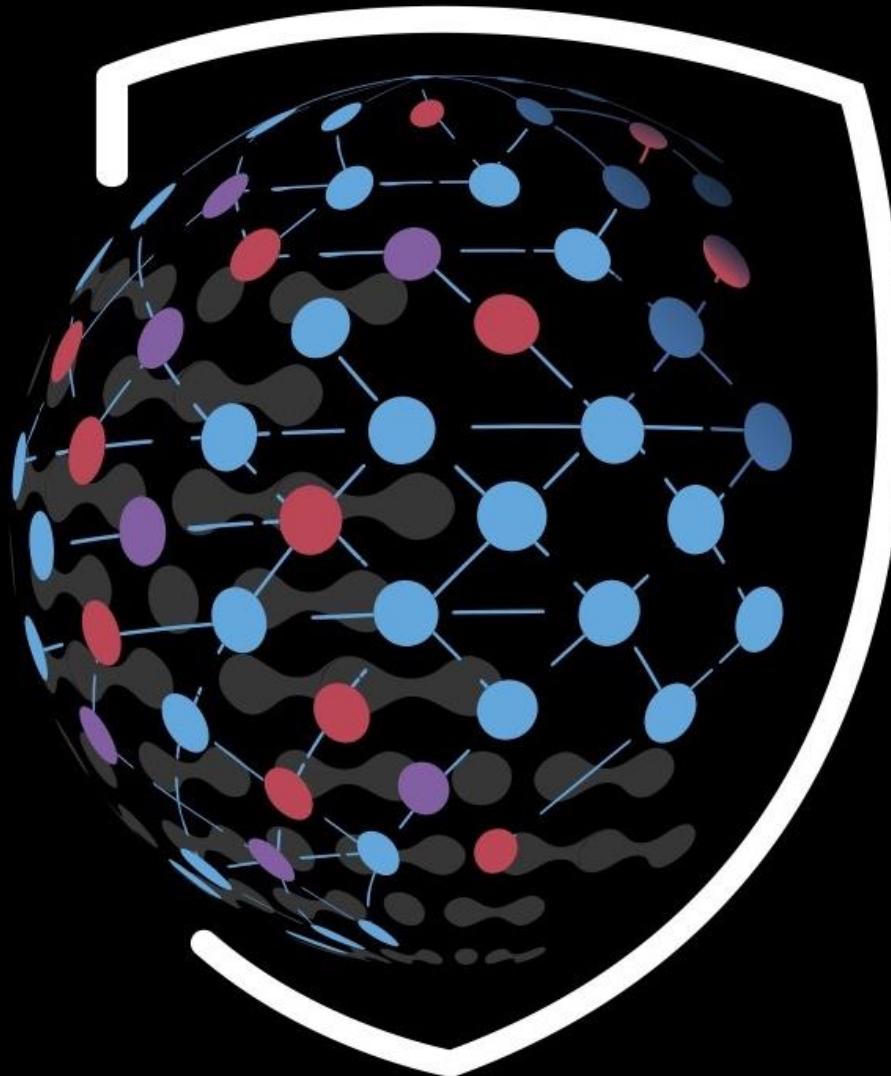
Project Spotlight: Open Threat Research

# Mordor & Mordor Datasets

## Intermission



\*\*\*\* Prepare your eyes for a white background slide deck \*\*\*



# OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY

# Roberto Rodriguez

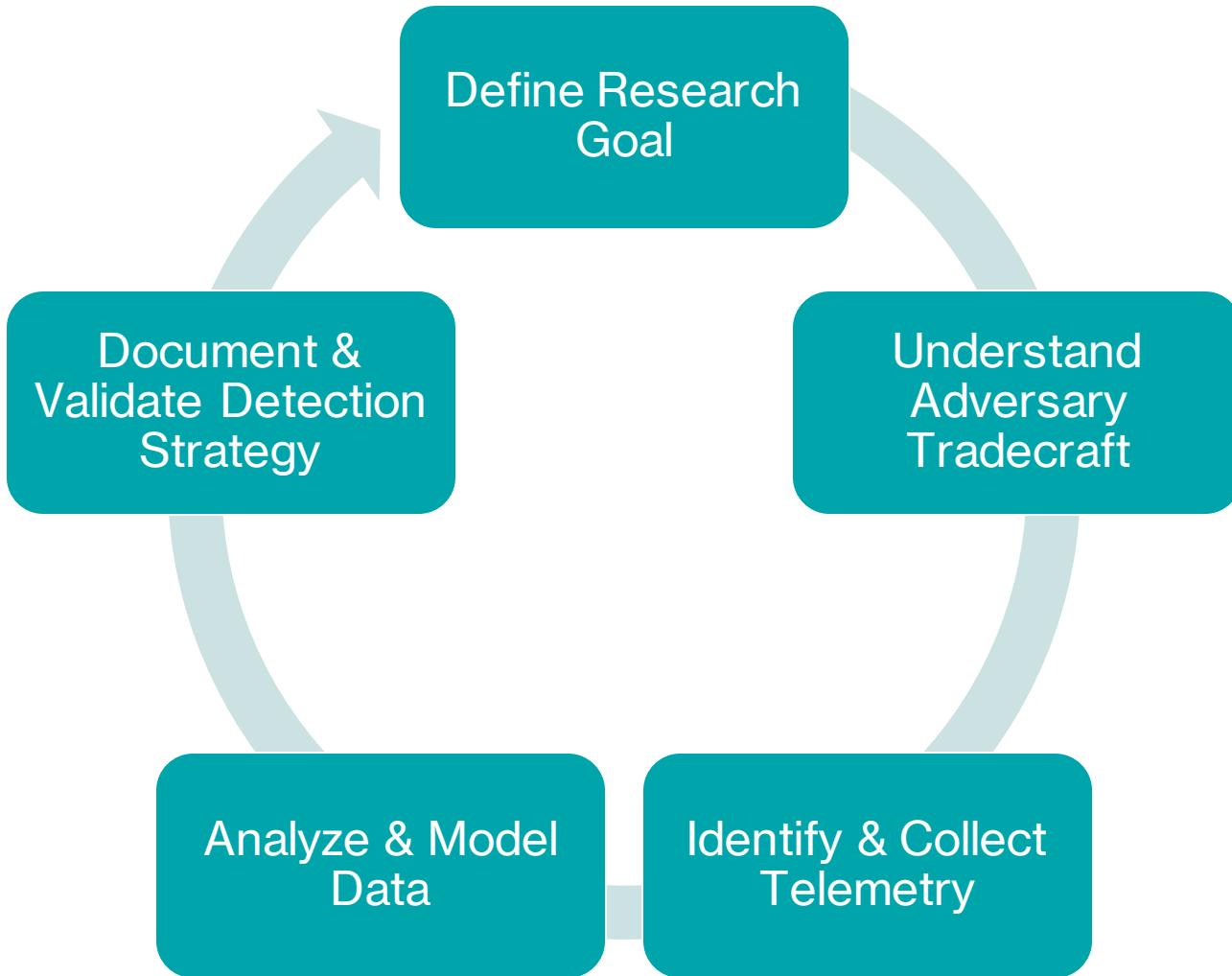
## @Cyb3rWard0g

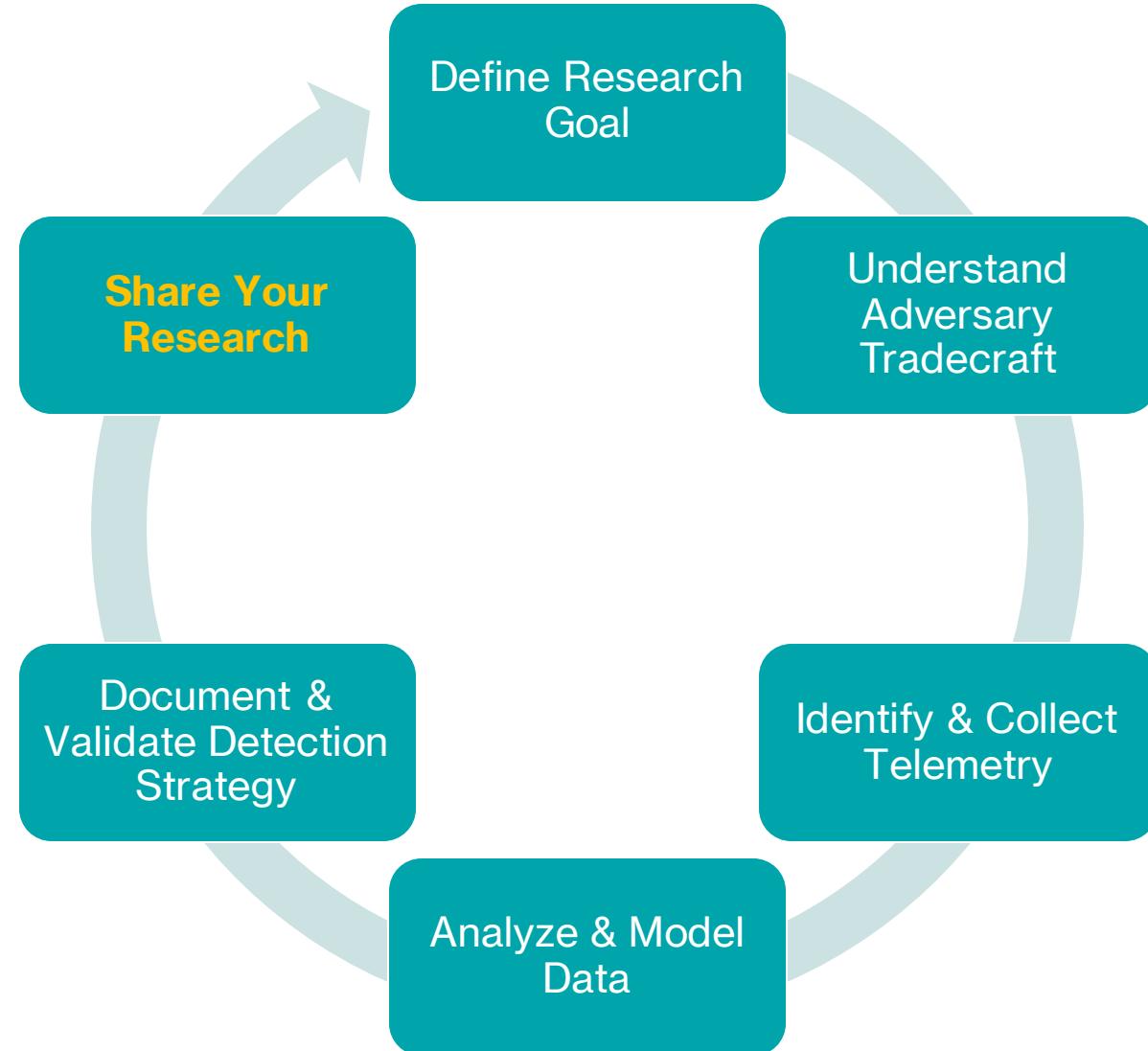
---

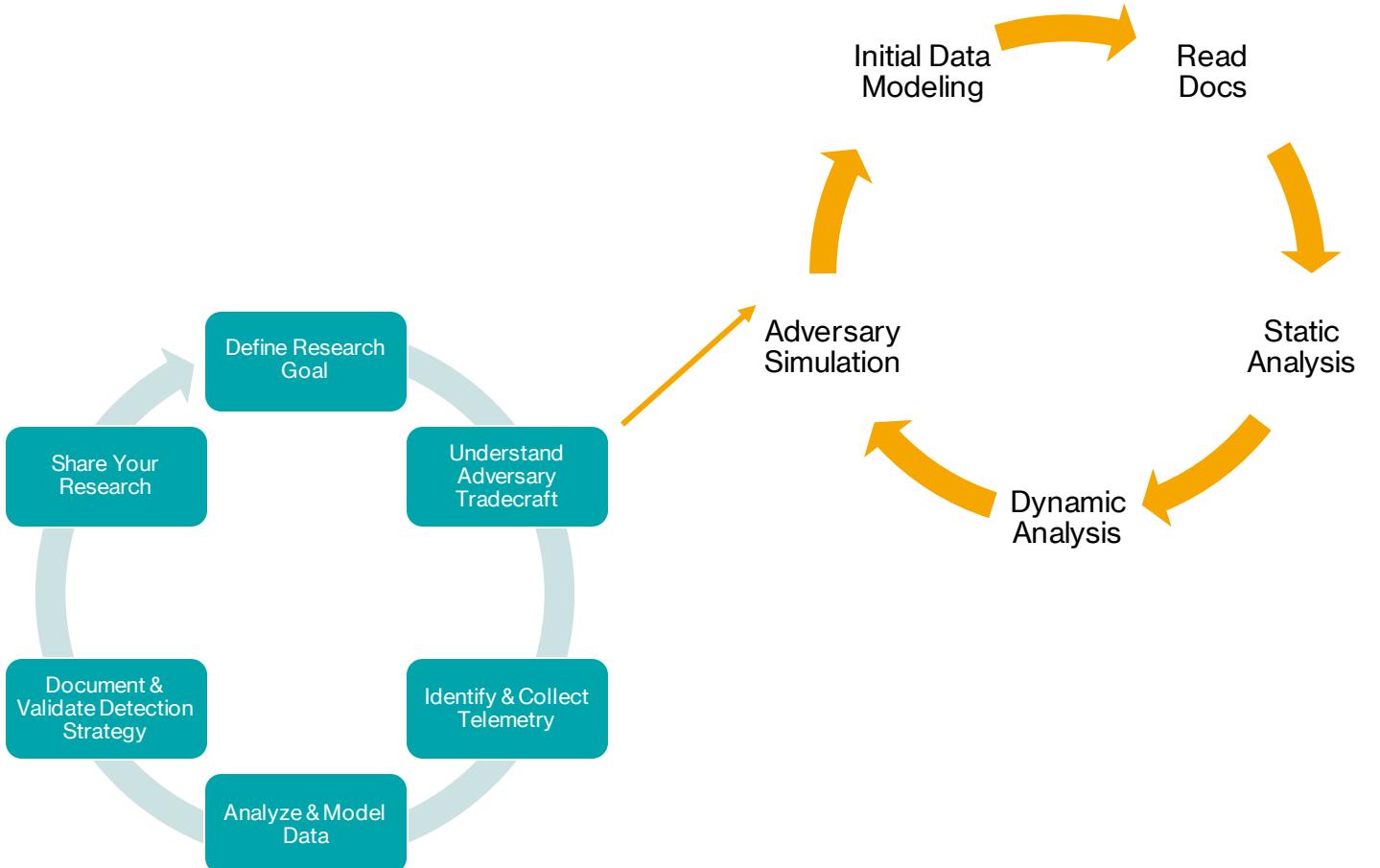
- Microsoft Threat Intelligence Center (MSTIC) R&D
- Open Source ❤
  - Threat Hunter Playbook [@HunterPlaybook](#)
  - Mordor [@Mordor\\_Project](#)
  - OSSEM [@OSSEM\\_Project](#)
  - Blacksmith & more..
- Open Threat Research Founder

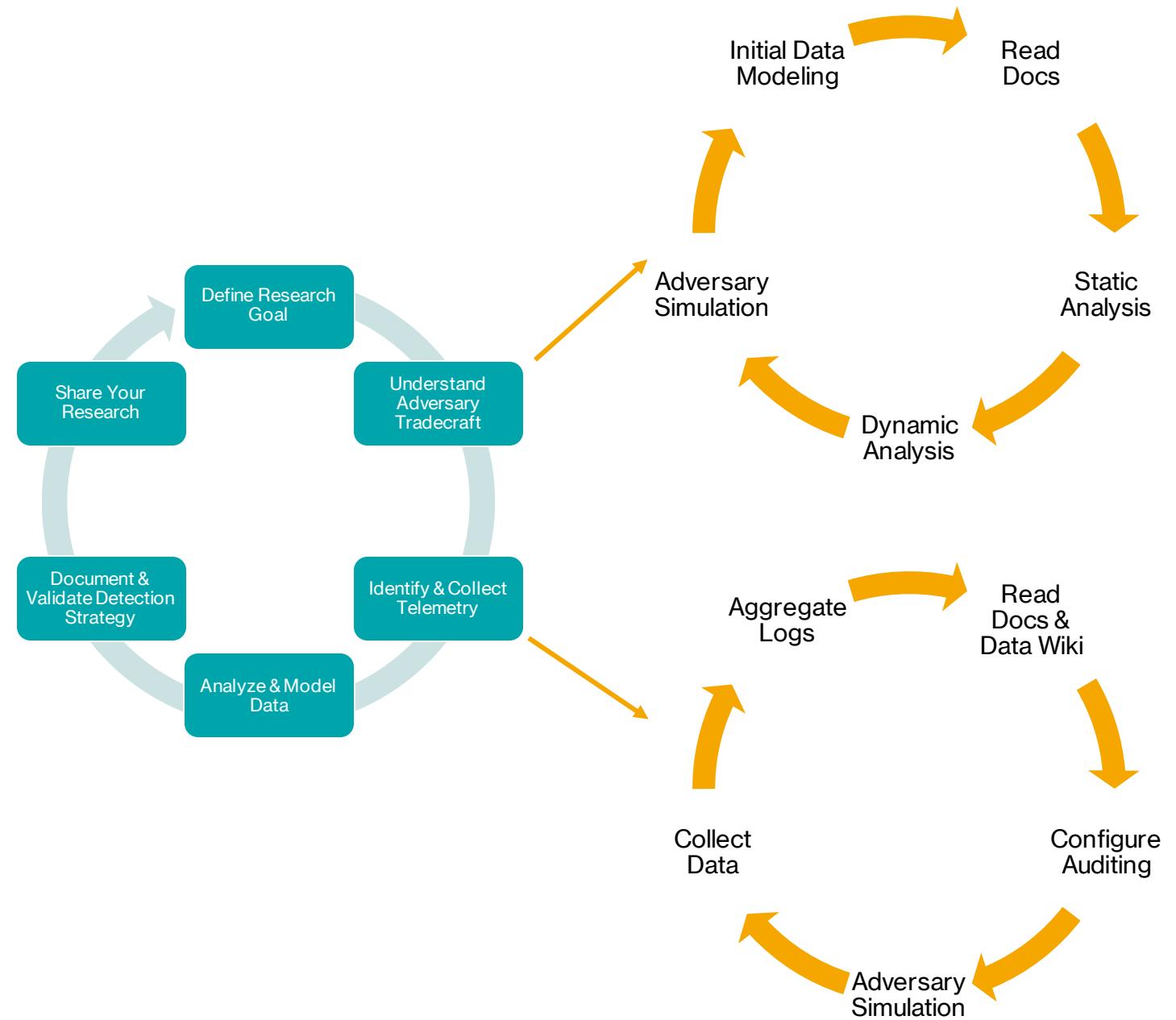


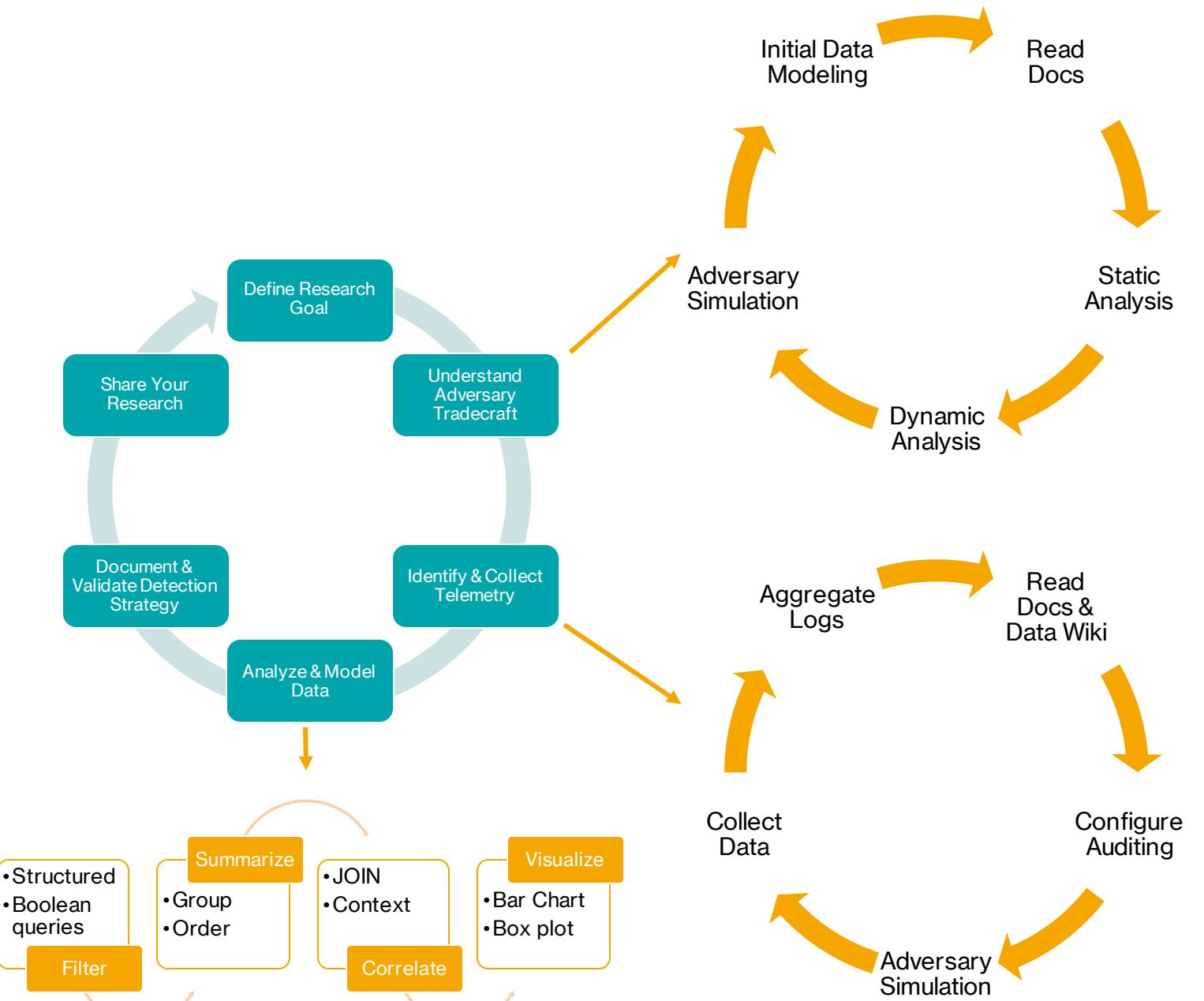
# Threat Research

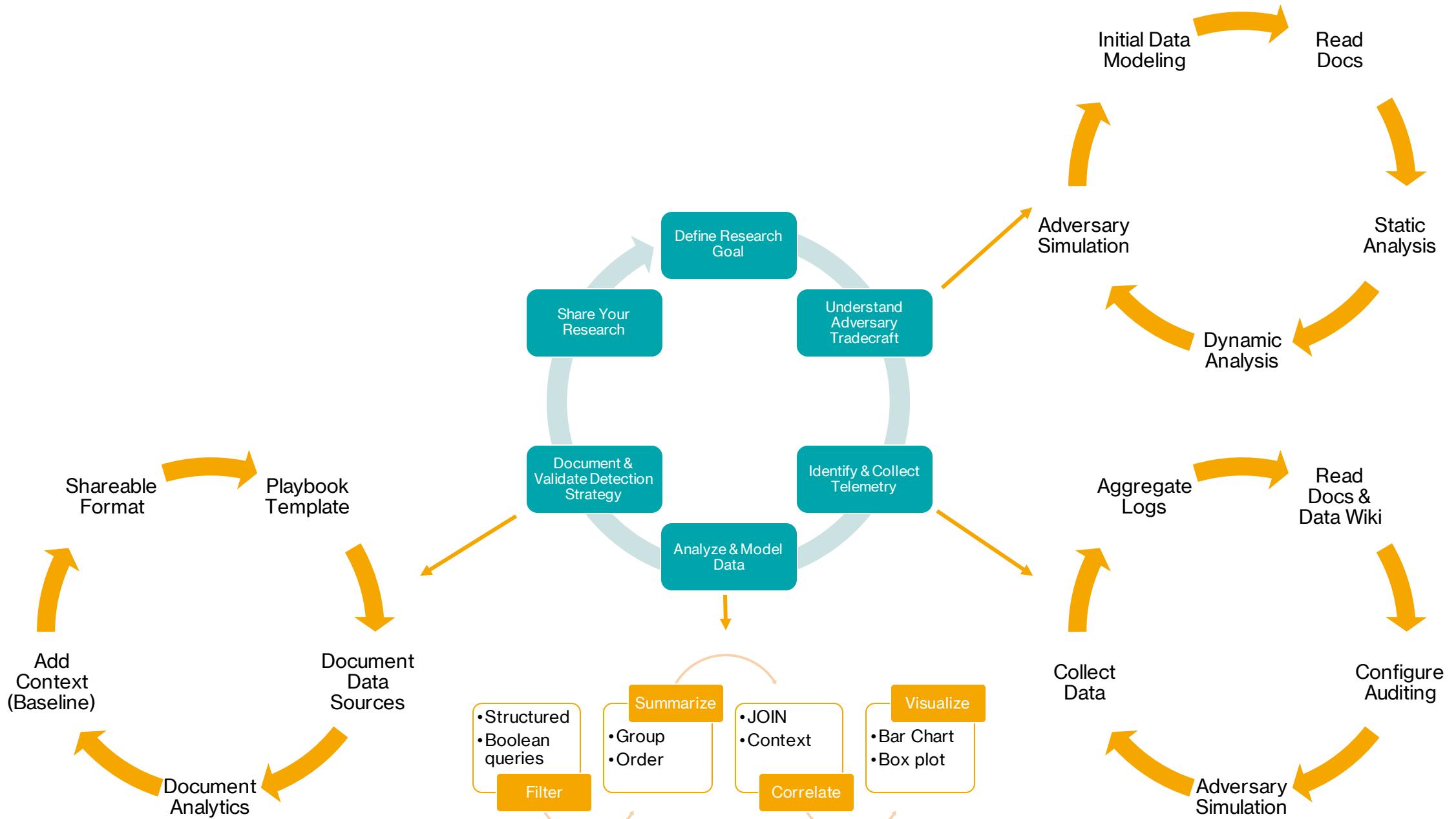


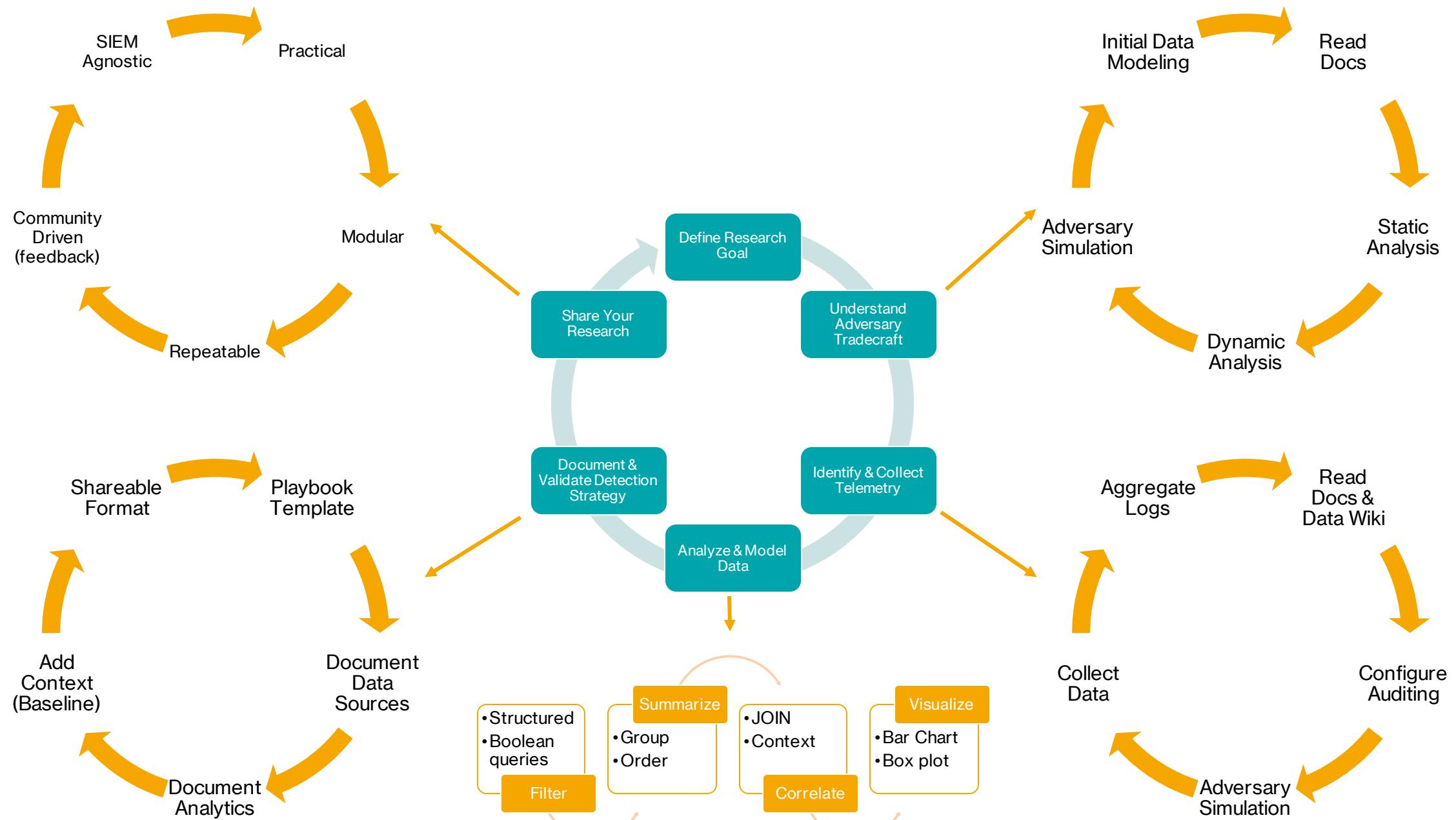


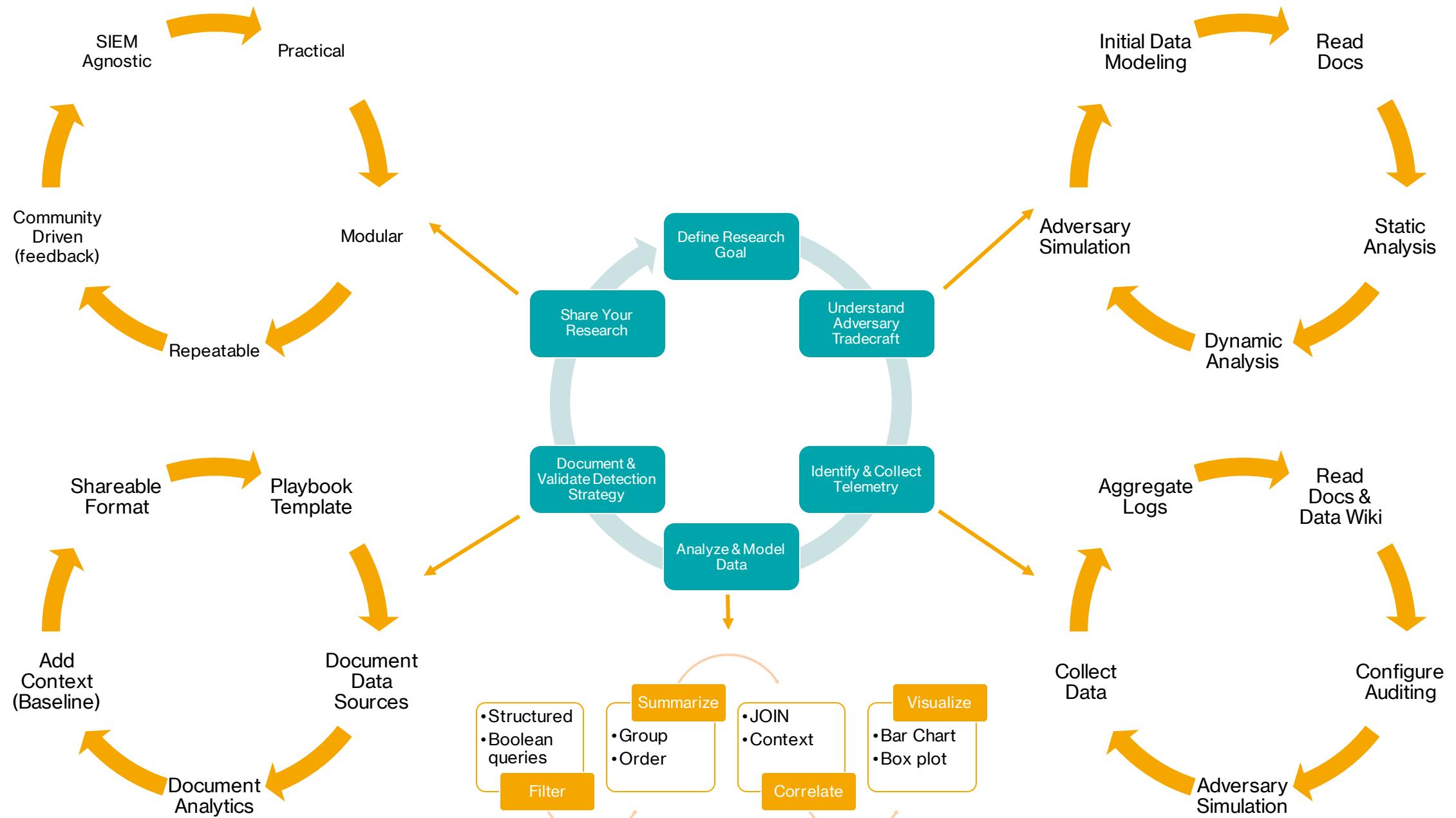




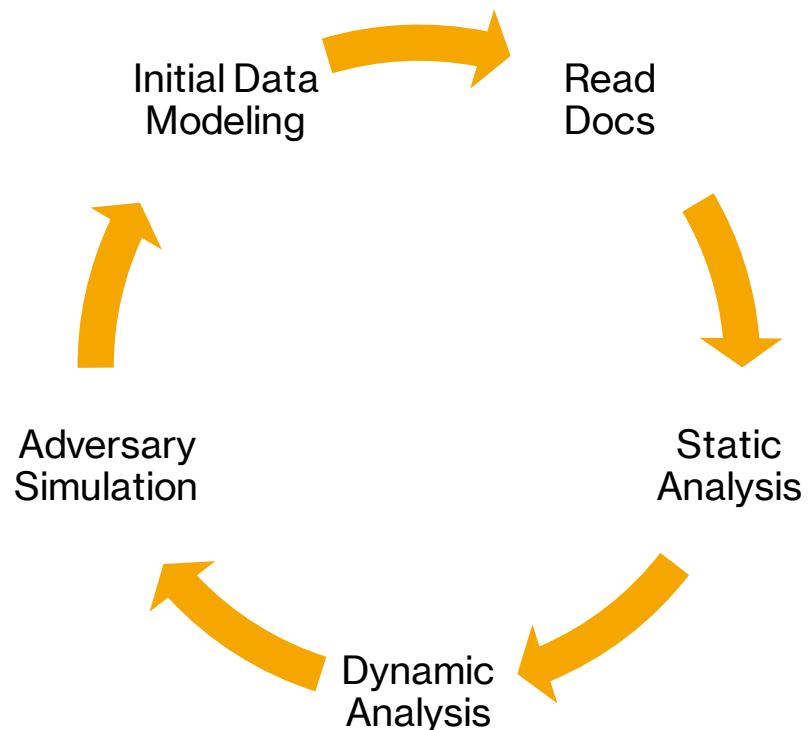




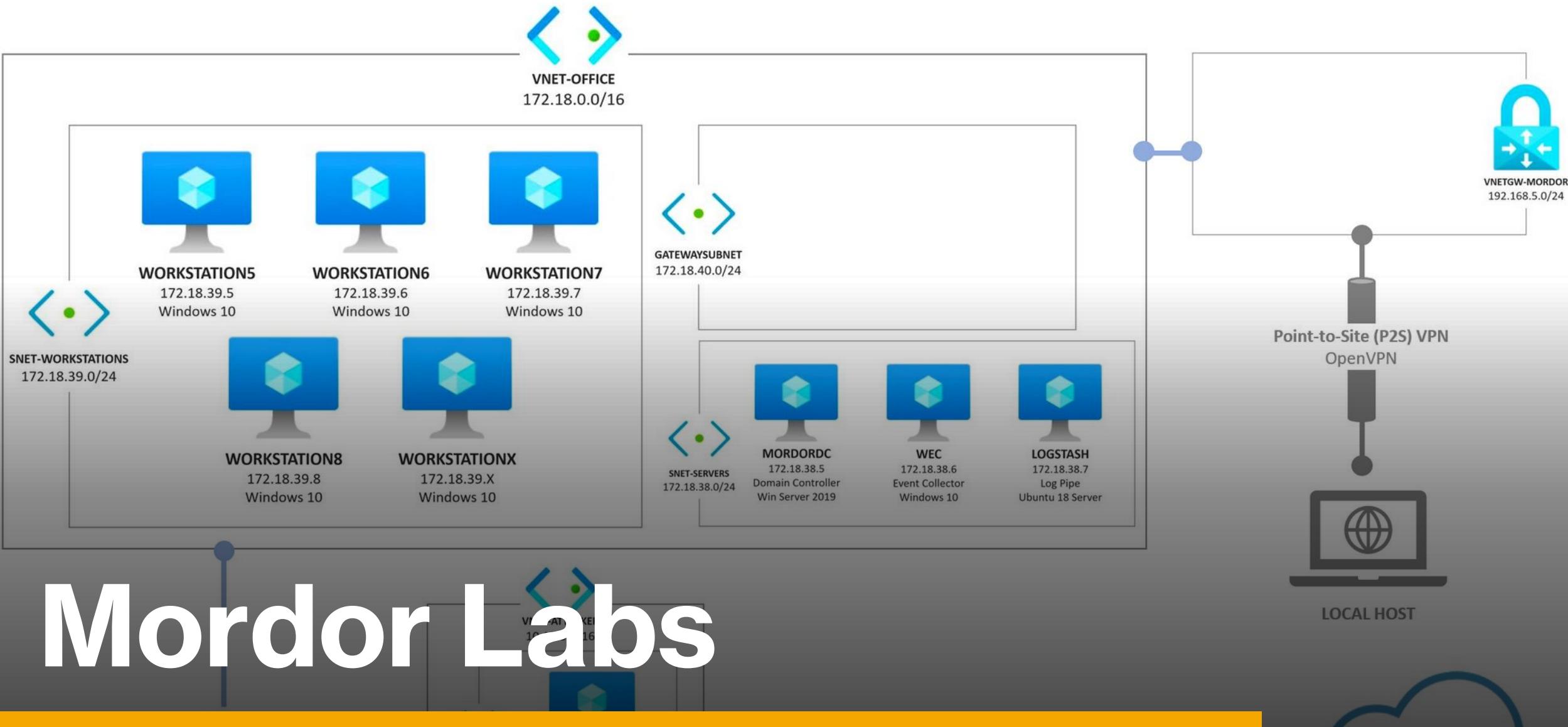




# Understand Adversary Tradecraft



- Read Docs
- Mordor Labs Project
- Mordor Project



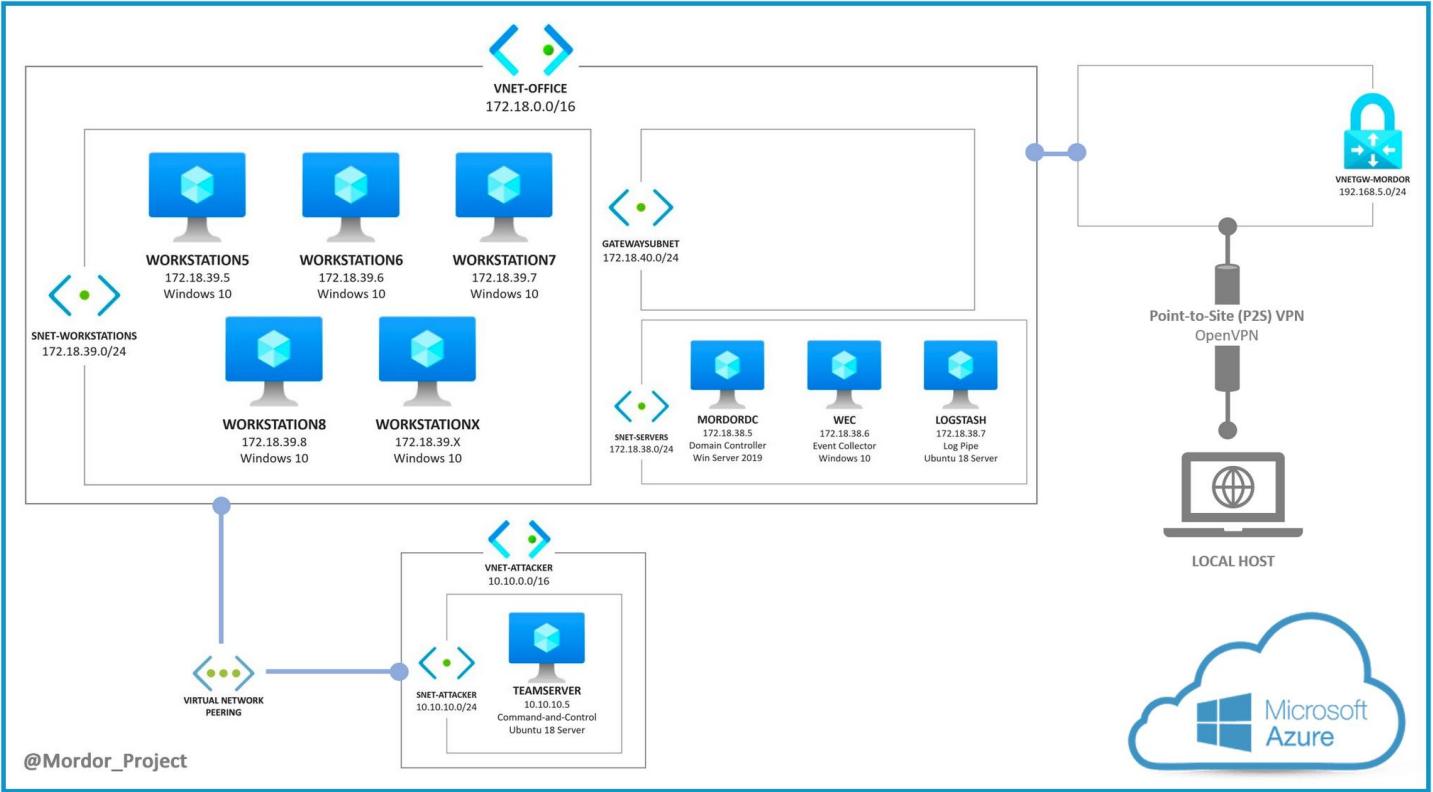
# Mordor Labs

# Mordor Labs

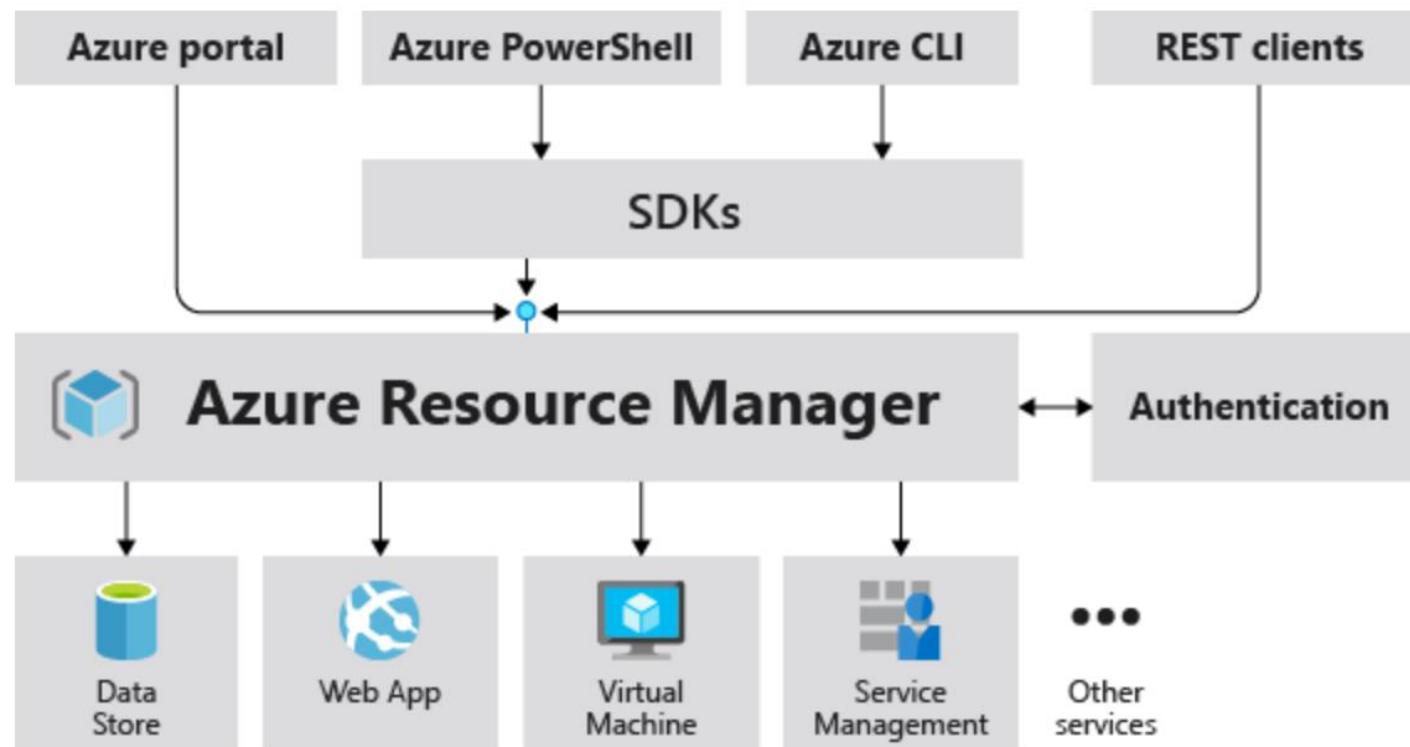


- A repository of cloud templates, configurations and scripts to deploy network environments **exclusively** to simulate adversaries and generate datasets for the Mordor project.
- **Environments:**
  - Windows
    - Shire
  - Linux
  - Cloud

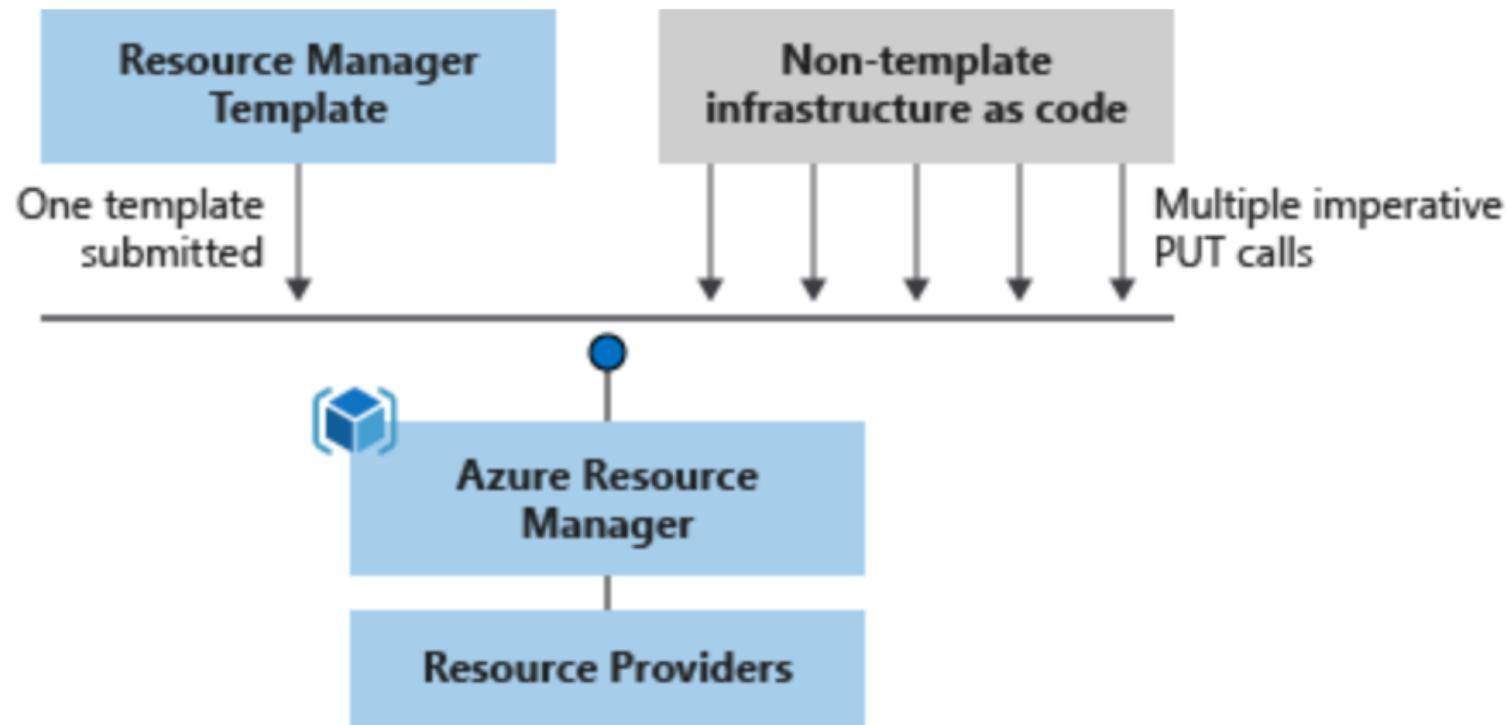
# Windows: The Shire



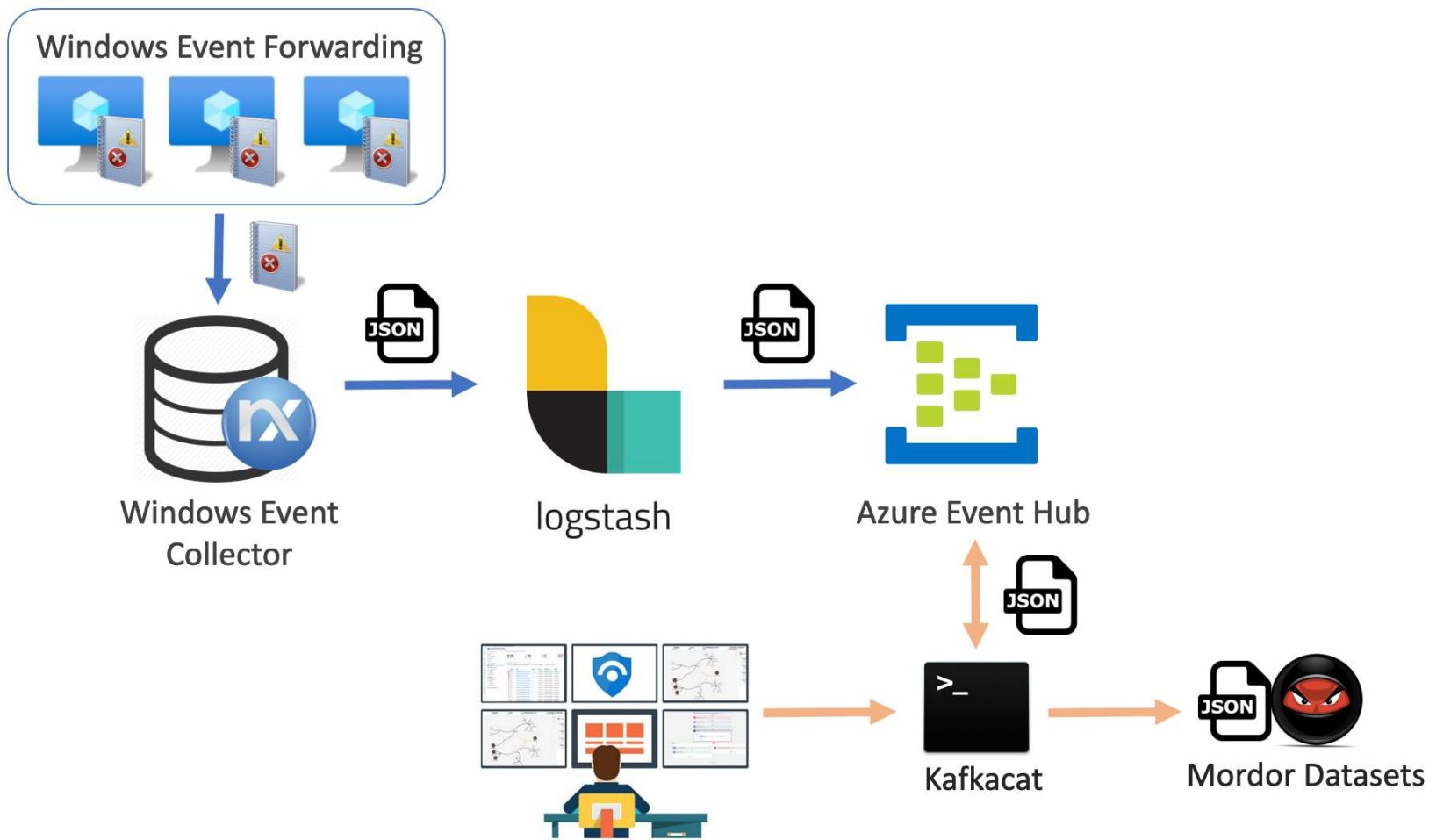
# Azure Resource Manager Service



# Azure Resource Manager Templates



# Windows Event Collection





OTRF / Blacksmith

<> Code Issues Pull requests 2 Actions Projects Wiki Security

master ▾ Blacksmith / resources / scripts / powershell / auditing /

Cyb3rWard0g Updated WEF and Prepare box script ..

Configure-WEC.ps1	Updated WEF and Prepare box script
Configure-WEF-Client.ps1	WinRM & Trusted Hosts
Enable-PowerShell-Logging.ps1	Updating PowerShell scripts
Enable-WinAuditCategories.ps1	Updating PowerShell scripts
Set-AuditSAMRemoteCalls.ps1	updated error handling
Set-SACLs.ps1	Updated Win Scripts SACL PrepareBox

# Windows Event Auditing

---



OTRF / Blacksmith

<> Code Issues Pull requests 2 Actions Projects Wiki Security

master ▾ Blacksmith / resources / scripts / powershell / auditing /

Cyb3rWard0g Updated WEF and Prepare box script

```
..      63 $ServiceRules = @"
  Config 64 service;addition
          "IKEEXT";"(AU;SAFA;RPWPDTCLC;;;WD)"
  Config 65 "SessionEnv";"S:(AU;SAFA;RPWPDTCLC;;;WD)"
          "scmanager";"(AU;SAFA;GA;;;NU)"
  Enabl 66 "@
  Enabl 67
  Set-A 68
  Set-S 69
  Set-S 70 $ServiceRules | ConvertFrom-Csv -Delimiter ';' | ForEach-Object {
    if(Get-Service $service){
        Write-Host "[+] Processing " $_.service
        # Get Sddl
        $sddl = (& $env:SystemRoot\System32\sc.exe sdshow $_.service | Out-String).Trim()
        # Define new Sddl
        $newSddl = ('{0}{1}' -f $sddl, $_.addition).Trim()
        # Update Sddl
        write-host "[>] Updating SDDL.."
        & $env:SystemRoot\System32\sc.exe sdset $_.service "$newSddl"
    }
}
```

# Windows Event Auditing

---

OTRF / Blacksmith

Code Issues Pull requests 2 Actions Projects Wiki Security

master Blacksmith / resources / configs / wef / subscriptions /

Cyb3rWard0g Updated WEF and Prepare box script

..

bits-client.xml	Updated WEF and Prepare box script
directory-service.xml	Updated WEF and Prepare box script
dns-client.xml	Updated WEF and Prepare box script
firewall-advanced-security.xml	Updated WEF and Prepare box script
powershell-operational.xml	Updated WEF and Prepare box script
powershell.xml	Updated WEF and Prepare box script
security.xml	Updated WEF and Prepare box script
sysmon.xml	Updated WEF and Prepare box script
system.xml	Updated WEF and Prepare box script
task-scheduler.xml	Updated WEF and Prepare box script
terminal-services.xml	Updated WEF and Prepare box script
wmi-activity.xml	Updated WEF and Prepare box script

# WEF Subscriptions

OTRF / Blacksmith

Code Issues Pull requests Actions Projects Wiki Security

master ▾

Blacksmith / resources / configs / wef / subscriptions /



Cyb3rWard11

bits-client.

directory-s

dns-client.

firewall-ad

powershell

powershell

security.xnr

sysmon.xrr

system.xm

task-schec

terminal-se

wmi-activit

```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
  <SubscriptionId>Sysmon</SubscriptionId>
  <SubscriptionType>SourceInitiated</SubscriptionType>
  <Description>Everything from the Microsoft-Windows-Sysmon/Operational channel</Description>
  <Enabled>true</Enabled>
  <Uri>http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
  <ConfigurationMode>Custom</ConfigurationMode>
  <Delivery Mode="Push">
    <Batching>
      <MaxItems>1</MaxItems>
      <MaxLatencyTime>100000</MaxLatencyTime>
    </Batching>
    <PushSettings>
      <Heartbeat Interval="900000"/>
    </PushSettings>
  </Delivery>
  <Query>
    <! [CDATA[
      <QueryList>
        <Query Id="0">
          <Select Path="Microsoft-Windows-Sysmon/Operational">*</Select>
        </Query>
      </QueryList>
    ]]>
  </Query>
  <ReadExistingEvents>true</ReadExistingEvents>
  <TransportName>http</TransportName>
  <ContentFormat>Events</ContentFormat>
  <Locale Language="en-US"/>
  <LogFile>ForwardedEvents</LogFile>
  <PublisherName>Microsoft-Windows-EventCollector</PublisherName>
  <AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>
  <!-- SDDL: Identifiers for "Domain Users" and "Domain Computers" -->
  <AllowedSourceDomainComputers>O:NG:BAD:P(A;;GA;;;DC)(A;;GA;;;DD)S:</AllowedSourceDomainComputers>
</Subscription>
```

# WEF Subscriptions

# Azure Event Hubs

Home >  
**evhns-MORDORi3sgm6cljcxza** Event Hubs Namespace

Search (Cmd+ /)  Refresh

+ Event Hub  Host name : evhns-MORDORi3sgm6cljcxza.servicebus.windows.net  
Tags (change) : Click here to add tags

NAMESPACE CONTENTS KAFKA SURFACE  
1 EVENT HUB ENABLED

Show metrics: Requests **Messages** Throughput  
For the last: 1 hour 6 hours 12 hours 1 day 7 days 31

Incoming Messages (Sum) Outgoing Messages (Sum) Captured Messages. (Sum)  
evhns-mordor3sgm6clj... evhns-mordor3sgm6clj... evhns-mordor3sgm6clj...  
**6.64k** 0 0

Search to filter items...

Name	Status	Message Retention	Partition Count
evh-mordor	Active	7 days	1

# Azure Event Hubs + Kafkacat

- **kafkacat** is a generic non-JVM producer and consumer for Apache Kafka >=0.8, think of it as a netcat for Kafka.
- In **producer** mode kafkacat reads messages from stdin, delimited with a configurable delimiter (-D, defaults to newline), and produces them to the provided Kafka cluster (-b), topic (-t) and partition (-p).
- In **consumer** mode kafkacat reads messages from a topic and partition and prints them to stdout using the configured message delimiter.

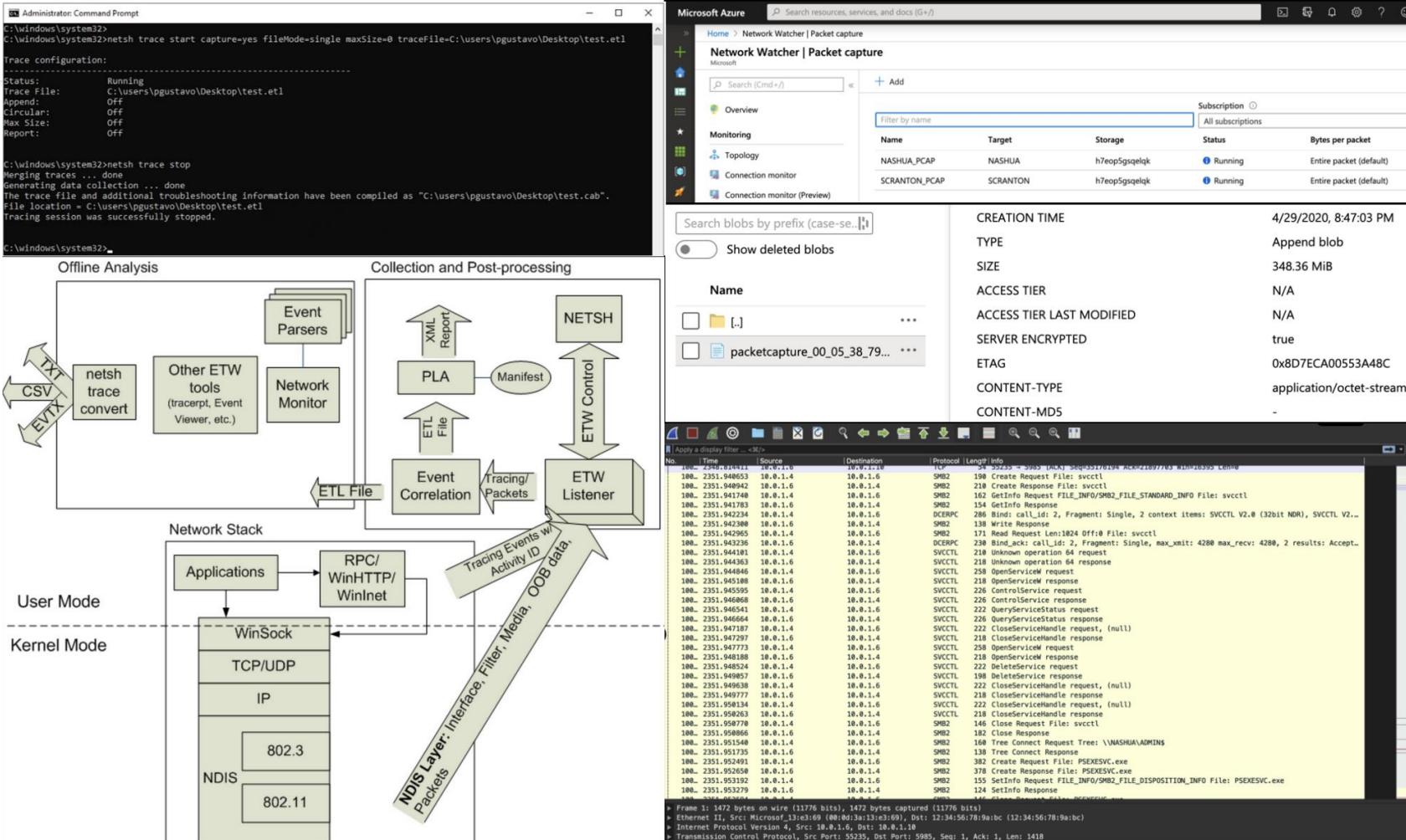
# Kafkacat: Consumer Mode!

```
kafkacat -b <AzureEventHub>:9093 -t  
evh-mordor -F kafkacat.conf -C -o end
```

# Kafkacat: Consumer Mode!

```
{"SourceName": "Microsoft-Windows-Security-Auditing", "port": 58178, "@timestamp": "2020-09-03T06:07:07.635Z", "version": "1", "OpcodeValue": 0, "RecordNumber": 49223, "Category": "Filtering Platform Connection", "Application": "\\\device\\harddiskvolume2\\windowsazure\\guestagent_2.7.41491.993_2020-09-03_025240\\waappagent.exe", "LayerName": "%1468%", "Message": "The Windows Filtering Platform has permitted a bind to a local port.\r\n\r\nApplication Information:\r\n\r\n\tProcess ID:\t\t3128\r\n\tApplication Name:\t\\device\\harddiskvolume2\\windowsazure\\guestagent_2.7.41491.993_2020-09-03_025240\\waappagent.exe\r\n\tNetwork Information:\r\n\t\tSource Address:\t\t0.0.0.0\r\n\t\tSource Port:\t\t51093\r\n\t\tProtocol:\t\t6\r\n\t\tFilter Information:\r\n\t\t\tFilter Run-Time ID:\t36", "Version": 0, "ExecutionProcessID": 4, "Protocol": "6", "Hostname": "WORKSTATION5.theshire.local", "LayerRTID": "36", "FilterRTID": "0", "ProviderGuid": "{54849625-5478-4994-ABBA-3E3B0328C300}", "ThreadID": 424, "Keywords": "-9214364837600034816", "EventReceivedTime": "2020-09-03 02:07:07", "tags": ["mordorDataset"], "SourceModuleType": "im_msvisatalog", "Severity": "INFO", "SourceAddress": "0.0.0.0", "SeverityValue": 2, "Task": 12818, "EventTime": "2020-09-03 02:07:05", "EventType": "AUDIT_SUCCESS", "Channel": "Security", "EventID": 51093, "SourcePort": "51093", "Opcode": "Info", "SourceModuleName": "eventlog", "ProcessId": "3128", "host": "wec.internal.cloudapp.net"}, {""ProcessId": "3128", "SourceName": "Microsoft-Windows-Security-Auditing", "port": 58178, "@timestamp": "2020-09-03T06:07:07.635Z", "version": "1", "OpcodeValue": 0, "RecordNumber": 49224, "Category": "Filtering Platform Connection", "Application": "\\\device\\harddiskvolume2\\windowsazure\\guestagent_2.7.41491.993_2020-09-03_025240\\waappagent.exe", "Direction": "%014593%", "LayerName": "%014611%", "Message": "The Windows Filtering Platform has permitted a connection.\r\n\r\nApplication Information:\r\n\r\n\tProcess ID:\t\t3128\r\n\tApplication Name:\t\\device\\harddiskvolume2\\windowsazure\\guestagent_2.7.41491.993_2020-09-03_025240\\waappagent.exe\r\n\tNetwork Information:\r\n\t\tDirection:\t\tOutbound\r\n\t\tSource Address:\t\t172.18.39.5\r\n\t\tSource Port:\t\t51093\r\n\t\tDestination Address:\t\t168.63.129.16\r\n\t\tDestination Port:\t\t80\r\n\t\tProtocol:\t\t6\r\n\t\tFilter Information:\r\n\t\t\tFilter Run-Time ID:\t71577", "Version": 1, "ExecutionProcessID": 4, "Protocol": "6", "Hostname": "WORKSTATION5.theshire.local", "DestPort": "80", "LayerRTID": "4B", "FilterRTID": "71577", "ProviderGuid": "{54849625-5478-4994-ABBA-3E3B0328C300}", "ThreadID": 424, "Keywords": "-9214364837600034816", "EventReceivedTime": "2020-09-03 02:07:07", "tags": ["mordorDataset"], "SourceModuleType": "im_msvisatalog", "Severity": "INFO", "SourceAddress": "172.18.39.5", "DestAddress": "168.63.129.16", "SeverityValue": 2, "Task": 12818, "EventTime": "2020-09-03 02:07:05", "EventType": "AUDIT_SUCCESS", "Channel": "Security", "EventID": 51093, "SourcePort": "51093", "Opcode": "Info", "RemoteUserID": "S-1-0-0", "RemoteMachineID": "S-1-0-0", "SourceModuleName": "eventlog", "host": "wec.internal.cloudapp.net"}  
cyb3rward0g@Roberto's-MBP lateral_movement %  
cyb3rward0g@Roberto's-MBP lateral_movement %  
cyb3rward0g@Roberto's-MBP lateral_movement %
```

# What about Network Telemetry?



The background image depicts a desolate, war-torn landscape. In the foreground, several soldiers wearing helmets and camouflage uniforms are crouching or lying on the ground, looking towards the horizon. Behind them, a city is shown in ruins, with tall, skeletal remains of buildings standing against a hazy sky. The overall mood is somber and suggests a scene from a historical or science-fiction setting.

# Mordor Datasets

# Mordor Datasets



- The Mordor project provides pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON) files for easy consumption and Packet Capture files
- Windows
- Linux
- Cloud

# Mordor Datasets



Consume Mordor Datasets

## EVENTS

Mordor Events!

## SMALL MORDOR DATASETS

### Windows

#### Execution

- Covenant Grunt Msbuild
- Empire Invoke PSRemoting
- Empire Invoke WMI Debugger
- Empire Invoke WMI
- Empire Invoke DCOM
- WMIC Add User Backdoor
- WMI Event Subscription
- Empire Invoke PsExec
- Empire Invoke Msbuild
- Empire Launcher VBS
- Covenant InstallUtil

#### Persistence

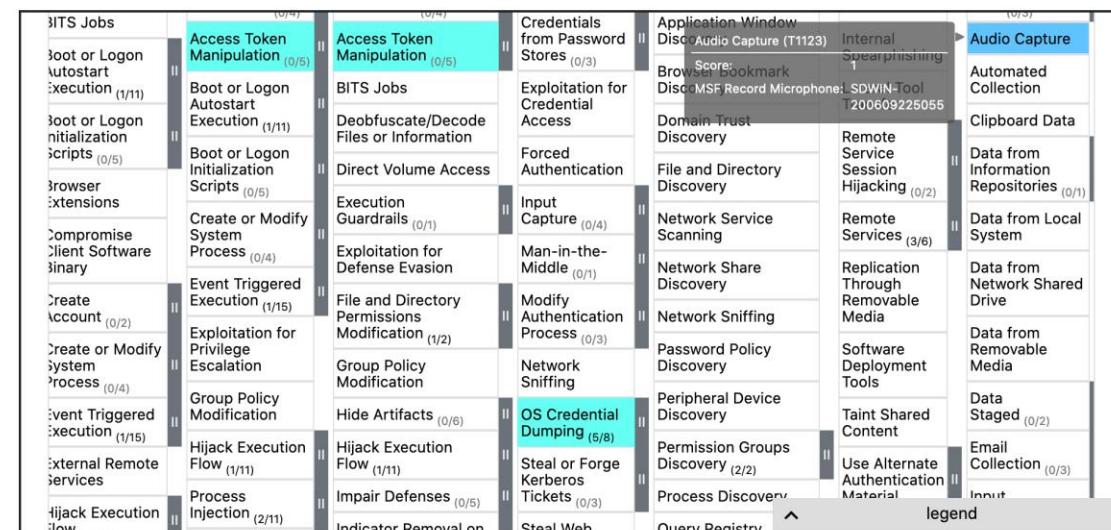
- Empire Userland Registry
- Empire Userland Scheduled Tasks
- Empire Elevated WMI Subscription
- Empire Elevated Scheduled Tasks
- SCM and DLL Hijacking IKEEXT
- Empire Elevated Registry

#### Privilege Escalation

- Empire Invoke Runas
- Empire Elevated WMI Subscription
- Empire DLL Injection

## Windows

### ATT&CK Navigator View



### ATT&CK Navigator View

Table View

### Table View

Created	Dataset	Description	Simulator	Author
---------	---------	-------------	-----------	--------

# Mordor Datasets : What can I do?

- Training
- Interviews
- Detection Hackathons
- Research
- Validate Analytics

# Mordor Datasets



## Threat Hunter Playbook

Search this book...

### PRE-HUNT ACTIVITIES

Data Management

### CAMPAIGN NOTEBOOKS

#### ATT&CK Evaluations

##### APT 29

Free Telemetry Report

[Free Telemetry Notebook](#)

### TARGETED NOTEBOOKS

Windows

Linux

Mac

### TUTORIALS

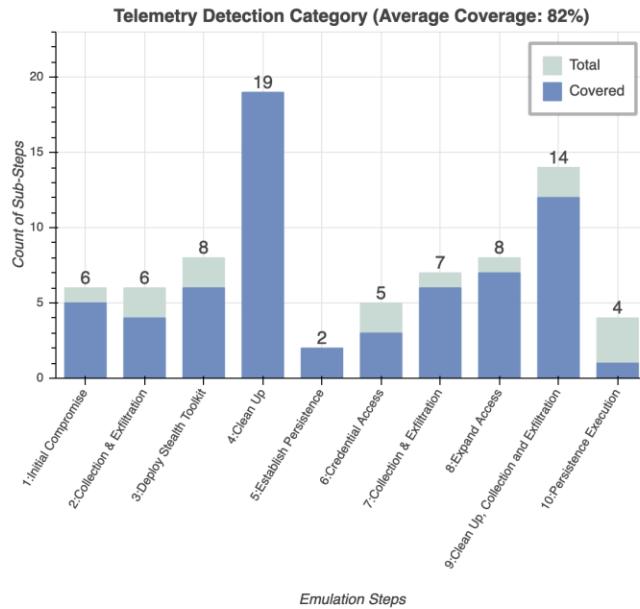
Jupyter Notebooks

## Telemetry Detection Category



Click to show +

BokehJS 2.1.0 successfully loaded.



Contents

### Telemetry Detection Category

Import Libraries

Start Spark Session

Decompress Dataset

Import Datasets

Create Temporary SQL View

Adversary - Detection Steps

1.A.1. User Execution

1.A.2. Masquerading

1.A.3. Uncommonly Used Port

1.A.4. Standard Cryptographic Protocol

1.B.1. Command-Line Interface

1.B.2. PowerShell

2.A.1. File and Directory Discovery

2.A.2. Automated Collection

2.A.3. Data from Local System

2.A.4. Data Compressed

2.A.5. Data Staged

2.B.1. Exfiltration Over Command and Control Channel

3.A.1. Remote File Copy

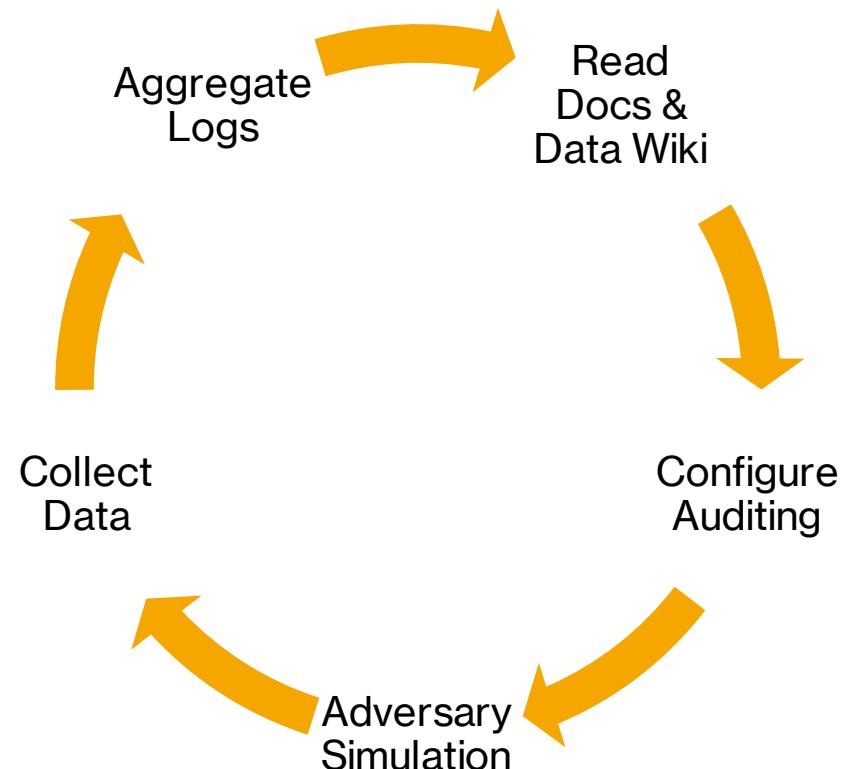
3.A.2. Obfuscated Files or Information

3.B.1. Component Object Model Hijacking

3.B.2. Bypass User Account Control

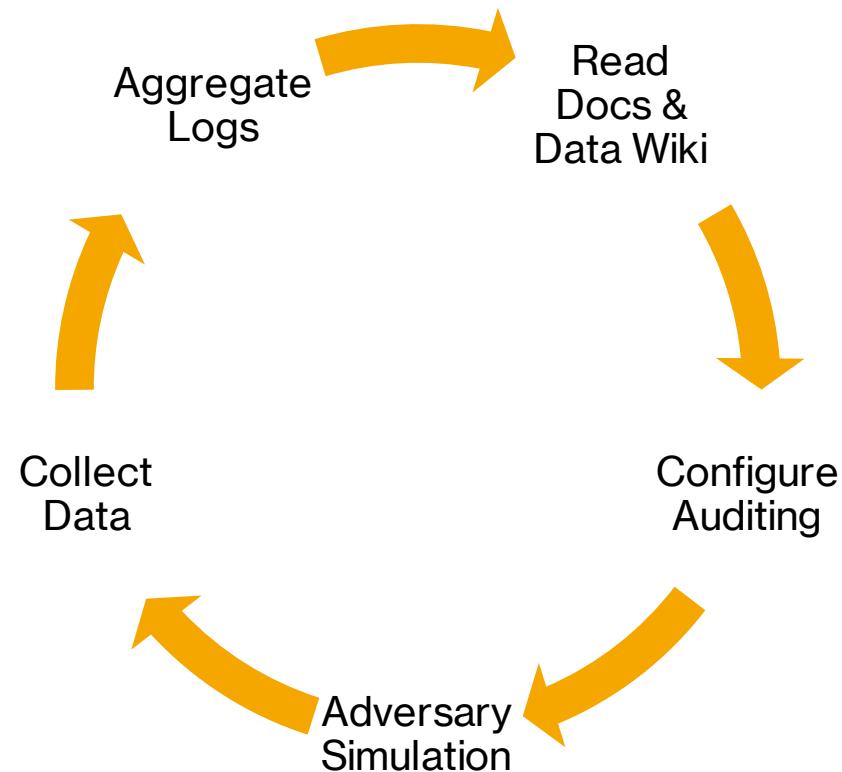
3.B.3. Commonly Used Port

# Identify & Collect Telemetry



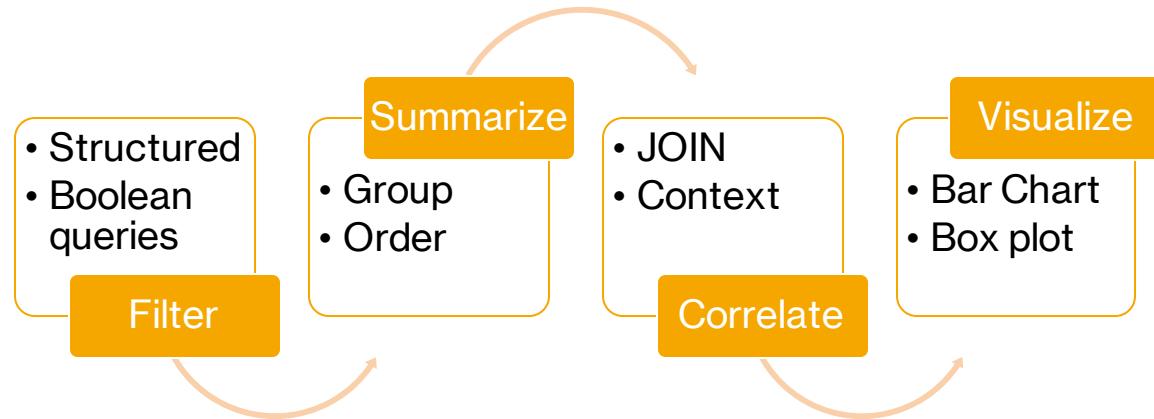
- Read Docs
- Community Data Wiki
- Community Common Data Model

# Identify & Collect Telemetry



- Centralize Logs
- Transform & Enrich Data
- Initial Data Exploration

# Analyze & Model Data

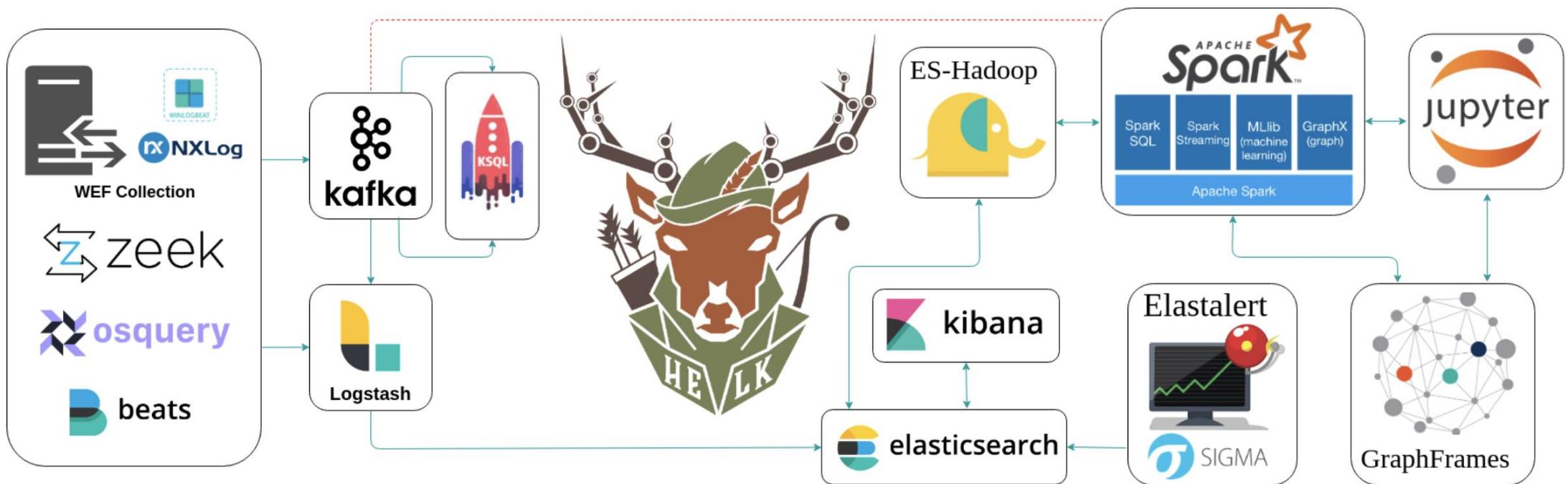


- Transform & Enrich Data
- Initial Data Exploration
- Jupyter Notebooks

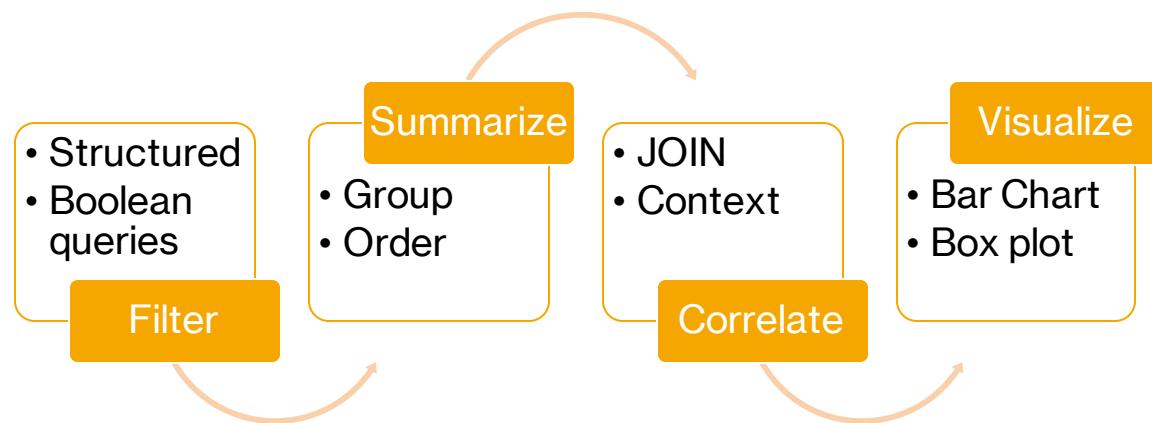
# HELK



# HELK



# Analyze & Model Data



- Data cleaning and transformation
- Statistical modeling
- Data visualization
- Machine learning, and much more

# What is a Jupyter Notebook?

- 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!)

# What is a Jupyter Notebook?

```
[Robertos-MacBook-Pro:~ wardog$ python3
Python 3.7.2 (default, Feb 12 2019, 08:16:38)
[Clang 10.0.0 (clang-1000.11.45.5)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> print('Hola Python!!')
Hola Python!!
>>> 12 * 2
24
>>>
```

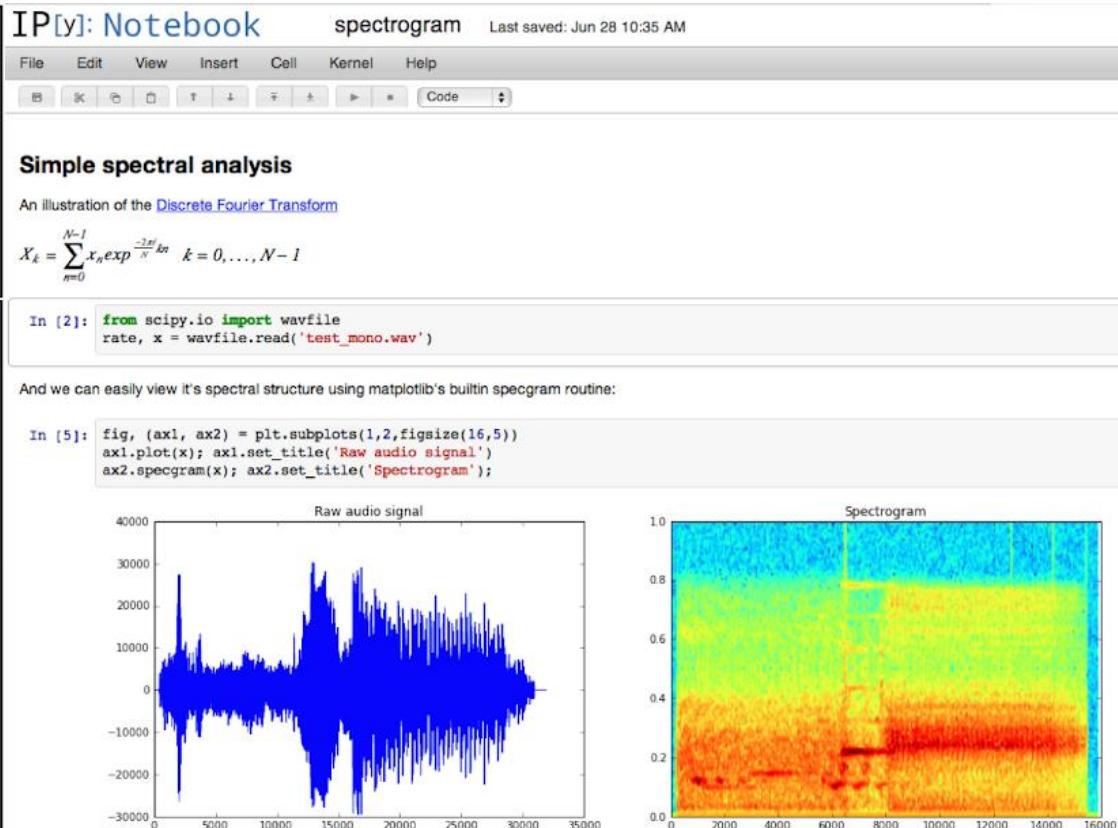
```
[Robertos-MacBook-Pro:GitHub wardog$ ipython
Python 2.7.10 (default, Oct 6 2017, 22:29:07)
Type "copyright", "credits" or "license" for more information.

IPython 5.7.0 -- An enhanced Interactive Python.
?          -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help       -> Python's own help system.
object?    -> Details about 'object', use 'object??' for extra details.

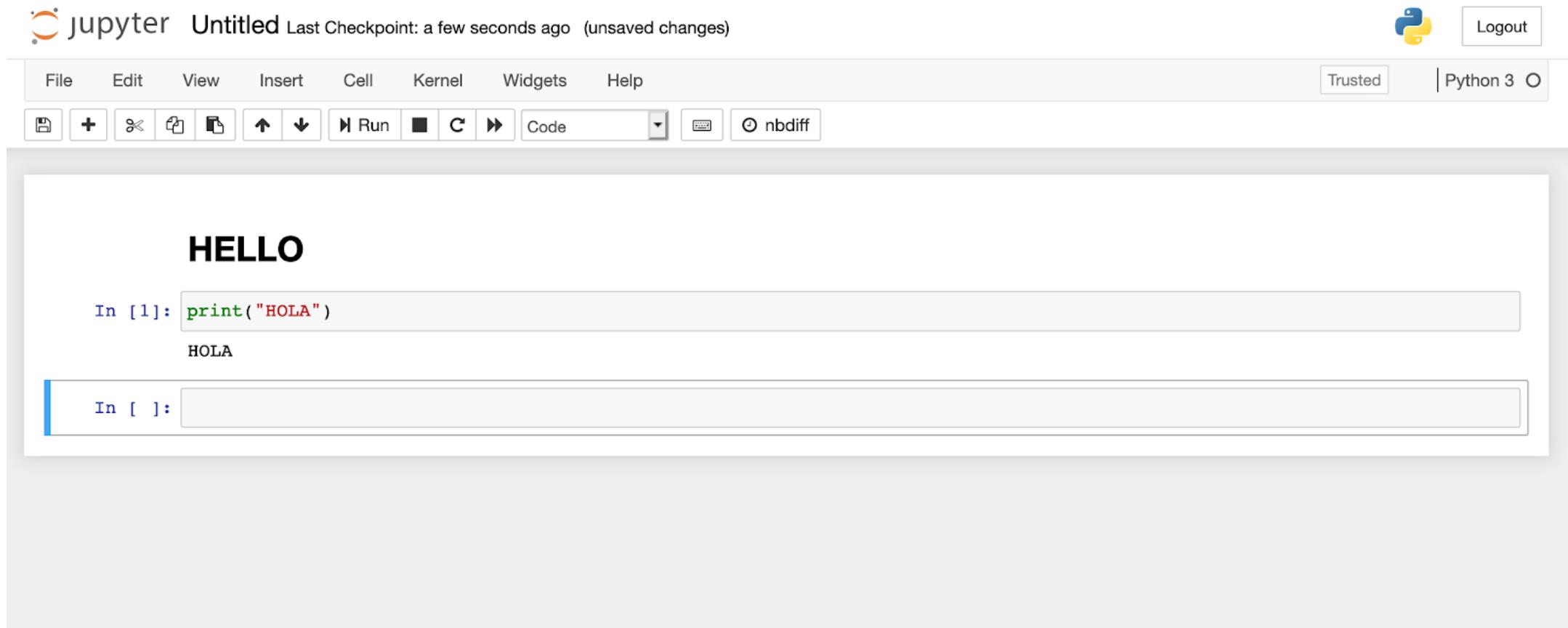
[In [1]: print('Hola IPython!!')
Hola IPython!!

[In [2]: 12 * 2
Out[2]: 24

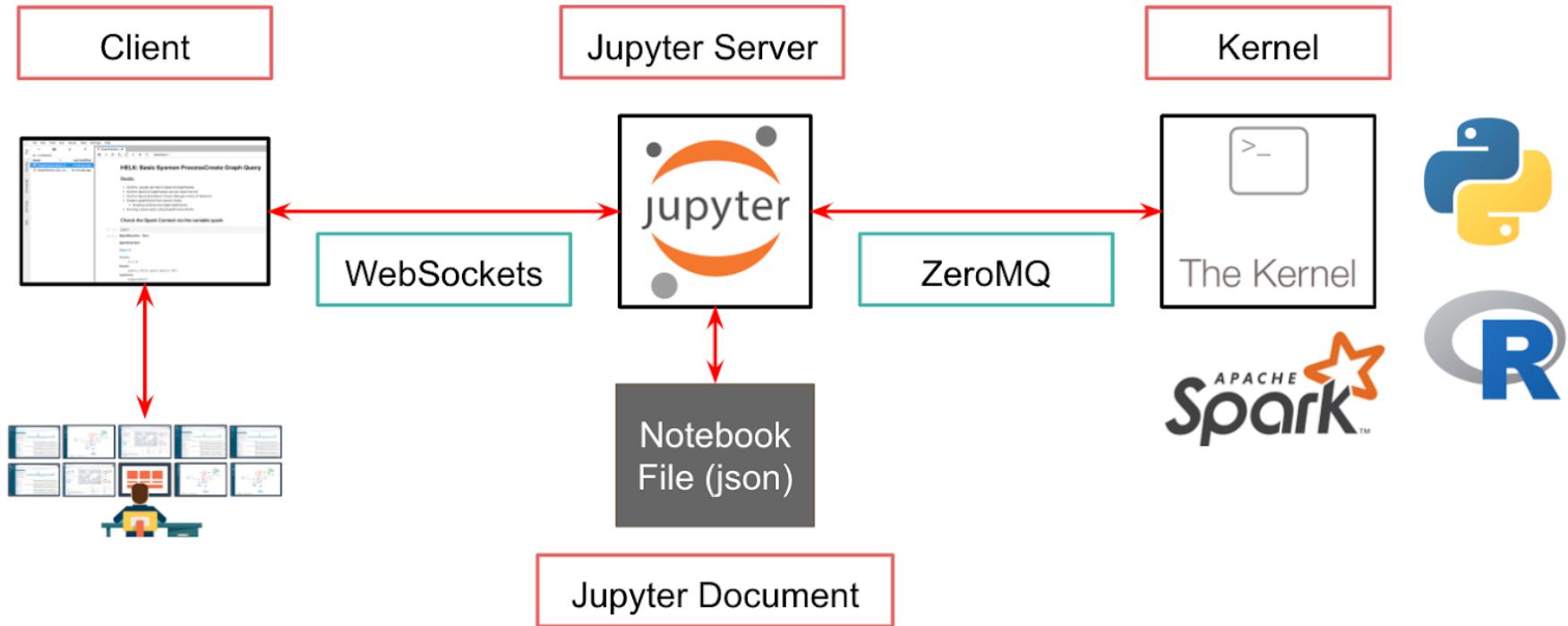
[In [3]:
```



# What is a Jupyter Notebook?



# Jupyter Notebook Architecture (Basics)



# What Can I Do?: Enrich Data

Installation

Fundamentals

Programming Languages

Libraries

Use Cases

Data Analysis

Data Connectors

Data Visualizations

Community Projects

Threat Hunter Playbook

Community Workshops

Defcon BTV 2020

Basic Data Analysis Concepts

Use Cases

Process Injection -  
CreateRemoteThread

DCSync dcerpc dcerpc

Remote Create Instance - dcerpc - wmi

Community Events

Infosec Jupyterthon



## Create a Spark UDF to get the specific Access Rights related to every Bitmask

- Define a function

```
def getSpecificAccessRights(bitmask):
    bitmask = int(bitmask,16)
    specificAccessRights = {'PROCESS_CREATE_PROCESS' : 0x0080,
                           'PROCESS_CREATE_THREAD' : 0x0002,
                           'PROCESS_DUP_HANDLE' : 0x0040,
                           'PROCESS_QUERY_INFORMATION' : 0x0400,
                           'PROCESS_QUERY_LIMITED_INFORMATION' : 0x1000,
                           'PROCESS_SET_INFORMATION' : 0x0200,
                           'PROCESS_SET_QUOTA' : 0x0100,
                           'PROCESS_SUSPEND_RESUME' : 0x0800,
                           'PROCESS_TERMINATE' : 0x0001,
                           'PROCESS_VM_OPERATION' : 0x0008,
                           'PROCESS_VM_READ' : 0x0010,
                           'PROCESS_VM_WRITE' : 0x0020,
                           'SYNCHRONIZE' : 0x00100000,
                           'PROCESS_SET_LIMITED_INFORMATION' : 0x2000}

    rights = [ ]

    for key,value in specificAccessRights.items():
        if value & bitmask != 0:
            rights.append(key)

    return rights
```

- Register Spark UDF

```
from pyspark.sql.types import *
spark.udf.register("getAccessRights", getSpecificAccessRights, ArrayType(StringType()))
```

```
<function __main__.getSpecificAccessRights(bitmask)>
```

On this page

[Creating SQL view from Mordor](#)

[Process Injection dataset](#)

[Filtering & Summarizing data](#)

Transforming data

[Create a Spark UDF to get the specific Access Rights related to every Bitmask](#)

[Filter events that requested "Creation of Thread" rights](#)

Correlating data

Thank you! I hope you enjoyed it!

# What Can I Do?: Filter & Summarize

- Apply the Spark UDF

```
processAccessRights = spark.sql(  
    """  
    SELECT GrantedAccess, getAccessRights(GrantedAccess) as RightsRequested, count(*) as Count  
    FROM processInjection  
    WHERE lower(Channel) LIKE '%sysmon%'  
        AND EventID = 10  
    GROUP BY GrantedAccess, RightsRequested  
    ORDER BY Count DESC  
    """)  
  
print('This dataframe has {} records!!'.format(processAccessRights.count()))  
processAccessRights.show(truncate = 80)
```

```
This dataframe has 10 records!!  
+-----+-----+  
|GrantedAccess| RightsRequeste  
+-----+-----+  
| 0x1000| [PROCESS_QUERY_LIMITED_INFORMATION  
| 0x3000| [PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_SET_LIMITED_INFORMATION  
| 0x40| [PROCESS_DUP_HANDLE  
| 0x1400| [PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION  
| 0x1410| [PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_VM_READ  
| 0x1478| [PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMA...  
| 0x1fffff| [PROCESS_CREATE_PROCESS, PROCESS_CREATE_THREAD, PROCESS_DUP_HANDLE, PROCESS_Q...  
| 0x1f3fff| [PROCESS_CREATE_PROCESS, PROCESS_CREATE_THREAD, PROCESS_DUP_HANDLE, PROCESS_Q...  
| 0x100000| [SYNCHRONIZE  
| 0x101541| [PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMA...
```

# What Can I Do?: Correlate

Find Source Processes that used CreateRemoteThread APIs

```
networkConnection = spark.sql(  
    ...  
    "SELECT b. SourceImage, b.TargetImage, a.NewThreadId  
    FROM processInjection b  
    INNER JOIN(  
        SELECT SourceProcessGUID, NewThreadId  
        FROM processInjection  
        WHERE lower(Channel) LIKE '%sysmon%'  
            AND EventID = 8  
    )a  
    ON b.SourceProcessGUID = a.SourceProcessGUID  
    WHERE lower(Channel) LIKE '%sysmon%'  
        AND b.EventID = 10  
        AND array_contains(getAccessRights(GrantedAccess), 'PROCESS_CREATE_THREAD')  
    ...)  
  
print('This dataframe has {} records!!'.format(networkConnection.count()))  
networkConnection.show(truncate = 40)
```

This dataframe has 88 records!!		
	SourceImage	TargetImage NewThreadId
C:\Windows\System32\WindowsPowerShell...	C:\Windows\system32\notepad.exe	3004
C:\Windows\System32\WindowsPowerShell...	C:\Windows\system32\notepad.exe	3756
C:\Windows\System32\WindowsPowerShell...	C:\Windows\system32\notepad.exe	2836
C:\Windows\System32\WindowsPowerShell...	C:\Windows\system32\notepad.exe	5764
C:\Windows\System32\WindowsPowerShell...	C:\Windows\system32\notepad.exe	8044
C:\Windows\System32\WindowsPowerShell...	C:\Windows\system32\notepad.exe	6168

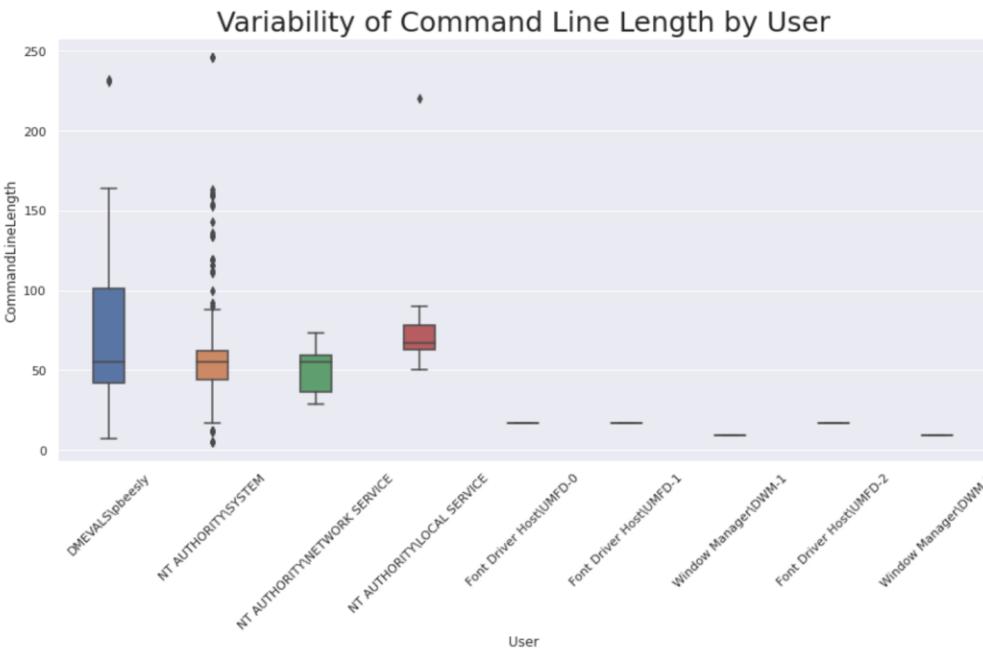
# What Can I Do?: Visualize

```
# Source of Data
source = commandLineLength.toPandas()

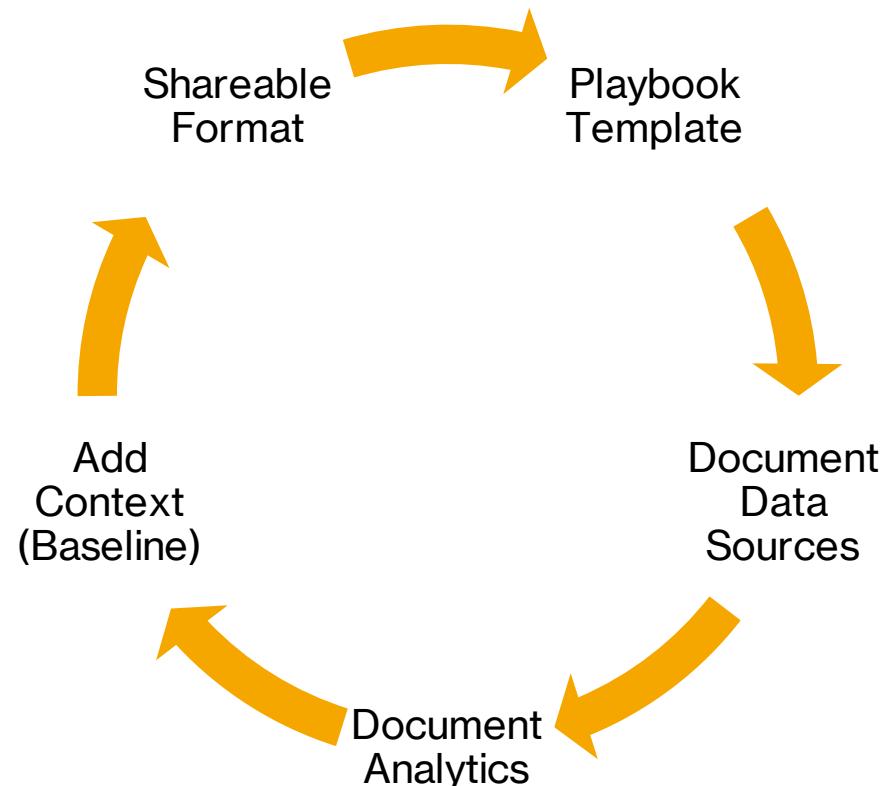
# seaborn object
boxPlotChart = sns.boxplot(x = 'User', y = 'CommandLineLength', data = source, orient = 'v',width=10)

# Title format
boxPlotChart.set_title("Variability of Command Line Length by User", fontsize = 25)

# X-axis format
boxPlotChart.set_xticklabels(boxPlotChart.get_xticklabels(), rotation=45);
```



# Document & Validate Detection



# Threat Hunter Playbook

# Document & Validate Detection

PRE-HUNT ACTIVITIES
Data Management
CAMPAIGN NOTEBOOKS
ATT&CK Evaluations
TARGETED NOTEBOOKS
<b>Windows</b>
Execution
Alternate PowerShell Hosts
WMI Win32_Process Class and Create
Method for Remote Execution
Basic PowerShell Execution
Service Creation
Alternate PowerShell Hosts
WMI Module Load
PowerShell Remote Session
PowerShell Remote Session
Persistence
WMI Eventing
Remote WMI
ActiveScriptEventConsumers
Privilege Escalation
Remote WMI
ActiveScriptEventConsumers
Defense Evasion
DLL Injection via
CreateRemoteThread and LoadLibrary
Enable Remote Desktop Connections
Registry
WDigest Downgrade

←

Windows

Contents

ATT&CK Navigator View

Table View

### ATT&CK Navigator View

The ATT&CK Navigator View for Windows displays a grid of attack techniques. Techniques are color-coded by category: grey for initial access, blue for persistence, red for defense evasion, and green for privilege escalation. Some techniques have a count of sub-techniques in parentheses.

Initial Access	Persistence	Defense Evasion	Privilege Escalation
Removable Media	Software Deployment Tools	Compromised Client Software Binary	System Process (0/4)
Supply Chain Compromise	Event Triggered Execution (T1546)	Create Account (0/2)	Event Triggered Execution (0/15)
Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Exploitation for Privilege Escalation
Valid Accounts (0/3)	Remote WMI ActiveScriptEventConsumers: WIN-20090202000000000000000000000000	User Execution (0/2)	Group Policy Modification
	Windows Management Instrumentation		Hijack Execution Flow (0/11)
			Process Injection (0/11)
			Hijack Execution Flow (0/11)
			Impair Defenses (0/5)
			Indicator Removal on Host (0/6)
			Indirect Command Execution
			Masquerading (0/6)
			Modify Authentication Process (0/3)
			Modify Registry
			Obfuscated File Information
			Scanning
			Network Share Discovery
			Network Sniffing
			File and Directory Permissions Modification (0/2)
			Group Policy Modification
			Hide Artifacts (0/6)
			OS Credential Dumping (0/8)
			Steal or Forge Kerberos Tickets (0/3)
			Query Registry
			Steal Web Session Cookie
			Two-Factor Authentication Interception
			Unsecured Credentials (0/5)
			Remote System Discovery
			Software Discovery (0/1)
			System Information Discovery
			System Network Discovery

### Table View

Created	Analytic	Hypothesis	Author
---------	----------	------------	--------

# Document & Validate Detection

CreateRemoteThread and LoadLibrary  
Enable Remote Desktop Connections  
Registry  
WDigest Downgrade  
Active Directory Replication User  
Backdoor  
Credential Access  
Domain DPAPI Backup Key Extraction  
SAM Registry Hive Handle Request  
Extended NetNTLM Downgrade  
Active Directory Replication From  
Non-Domain-Controller Accounts  
Remote Interactive Task Manager  
LSASS Dump  
LSASS Access from Non System Account  
Discovery  
SAM Registry Hive Handle Request  
SysKey Registry Keys Access  
Remote Service Control Manager Handle  
**Lateral Movement**  
Remote Service creation  
WMI Win32\_Process Class and Create Method for Remote Execution  
**Remote WMI**  
**ActiveScriptEventConsumers**  
PowerShell Remote Session Collection  
Access to Microphone Device  
Linux

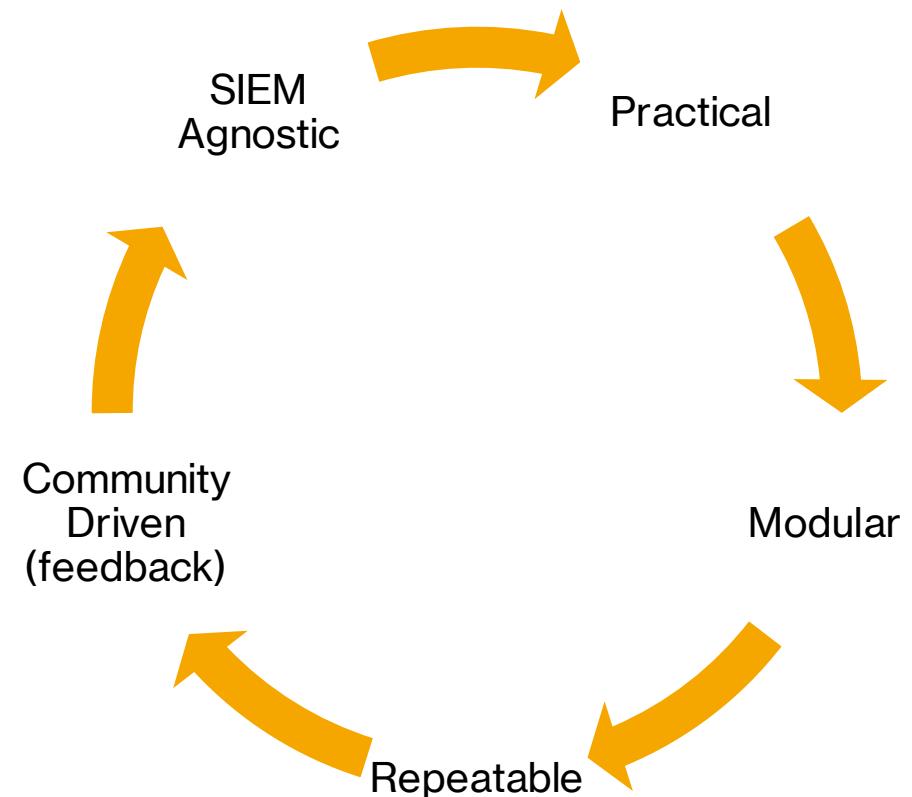
```
df = spark.sql(  
    '''  
SELECT d.`@timestamp`, d.TargetUserName, c.Image, c.ProcessId  
FROM mordorTable d  
INNER JOIN (  
    SELECT b.ImageLoaded, a.CommandLine, b.ProcessGuid, a.Image, b.ProcessId  
    FROM mordorTable b  
    INNER JOIN (  
        SELECT ProcessGuid, CommandLine, Image  
        FROM mordorTable  
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 1  
        AND Image LIKE '%scrcons.exe'  
    ) a  
    ON b.ProcessGuid = a.ProcessGuid  
    WHERE b.Channel = "Microsoft-Windows-Sysmon/Operational"  
    AND b.EventID = 7  
    AND LOWER(b.ImageLoaded) IN (  
        'c:\\\\windows\\\\system32\\\\wbem\\\\scrcons.exe',  
        'c:\\\\windows\\\\system32\\\\\\\\vbscript.dll',  
        'c:\\\\windows\\\\system32\\\\wbem\\\\wbemdisp.dll',  
        'c:\\\\windows\\\\system32\\\\wshom.ocx',  
        'c:\\\\windows\\\\system32\\\\scrun.dll'  
    )  
    ) c  
ON split(d.ProcessId, '0x')[1] = LOWER(hex(CAST(c.ProcessId as INT)))  
WHERE LOWER(d.Channel) = "security"  
    AND d.EventID = 4624  
    AND d.LogonType = 3  
    ''')  
df.show(10, False)
```

@timestamp	TargetUserName	Image	ProcessId
2020-09-02T01:44:11.726Z	pgustavo	C:\Windows\System32\wbem\scrcons.exe	972
2020-09-02T01:44:11.726Z	pgustavo	C:\Windows\System32\wbem\scrcons.exe	972
2020-09-02T01:44:11.726Z	pgustavo	C:\Windows\System32\wbem\scrcons.exe	972
2020-09-02T01:44:11.726Z	pgustavo	C:\Windows\System32\wbem\scrcons.exe	972
2020-09-02T01:44:11.726Z	pgustavo	C:\Windows\System32\wbem\scrcons.exe	972

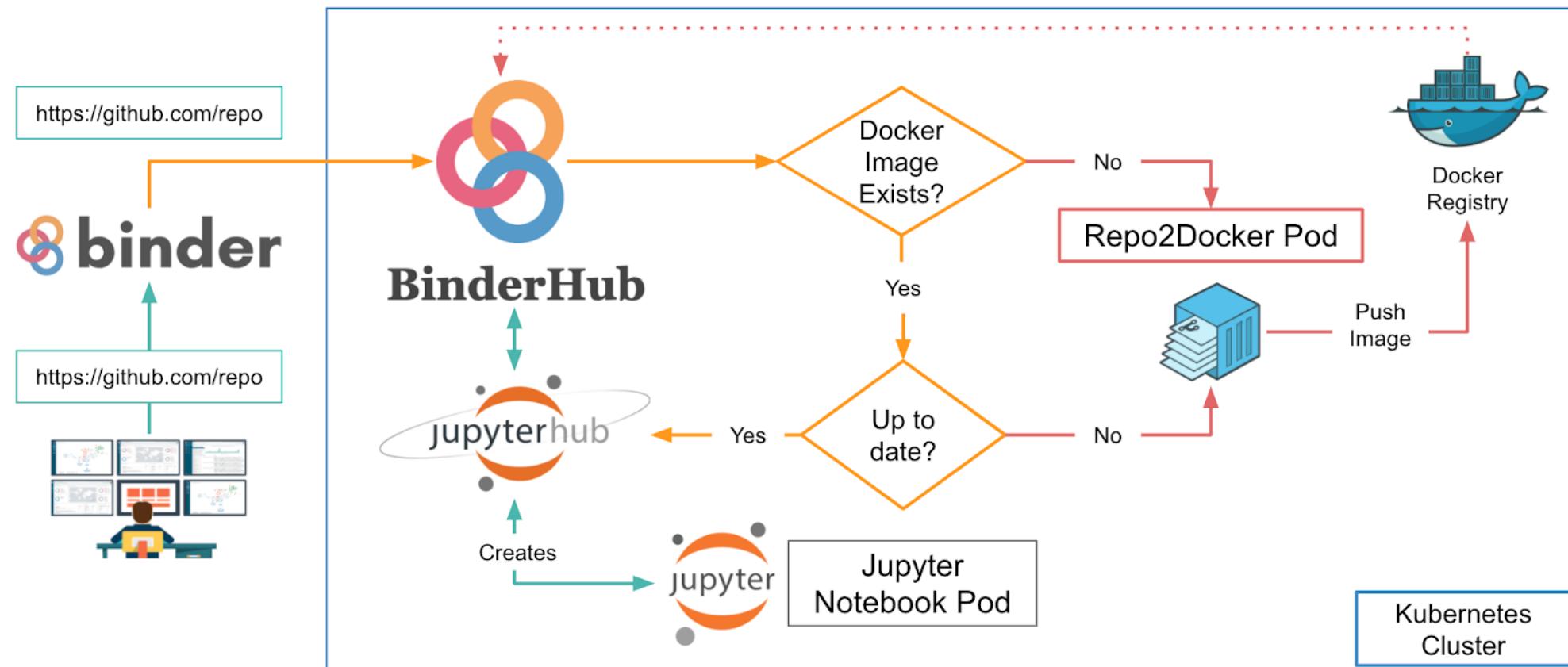
## Contents

Metadata  
Technical Description  
Hypothesis  
**Analytics**  
Initialize Analytics Engine  
Download & Process Mordor  
File  
Analytic I  
Analytic II  
Analytic III  
Analytic IV  
Analytic V  
Analytic VI  
**Analytic VII**  
Analytic VIII  
Detection Blindspots  
Hunter Notes  
Hunt Output  
References

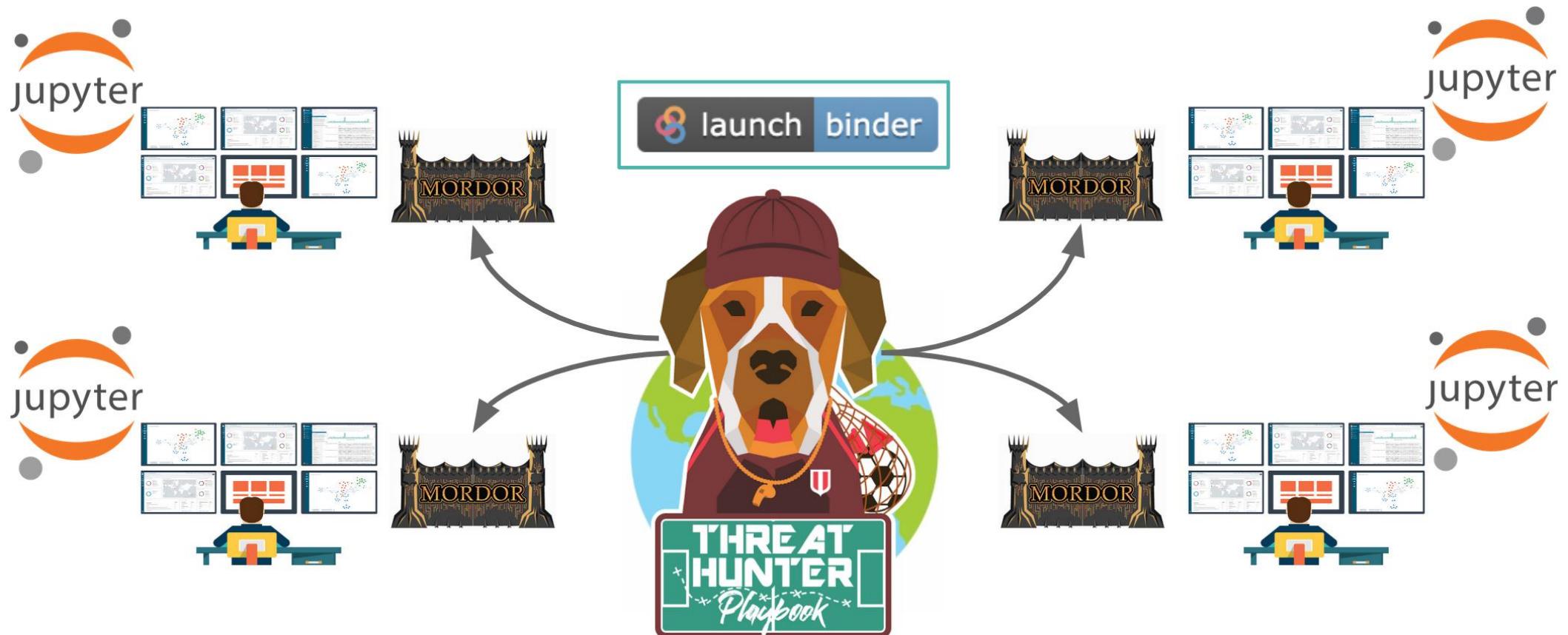
# Share Your Research!



# Repeatable? Practical? SIEM Agnostic?



# Repeatable? Practical? SIEM Agnostic?



# Repeatable? Practical? SIEM Agnostic?

 ThreatHunter-Playbook @HunterPlaybook · 17h  
"Adversaries might be leveraging WMI event subscriptions (ActiveScriptEventConsumers) for remote code execution"  
@OTR\_Community 🌎

📅 Playbook: [threathunterplaybook.com/notebooks/wind...](https://threathunterplaybook.com/notebooks/wind...)

😈 @Mordor\_Project datasets: [mordordatasets.com/notebooks/smal...](https://mordordatasets.com/notebooks/smal...)

🔔 Reference: @domchell [mdsec.co.uk/2020/09/i-like...](https://mdsec.co.uk/2020/09/i-like...)



Remote WMI ActiveScriptEventConsumers  
Remote WMI ActiveScriptEventConsumers Metadata  
id WIN-200902020333 author Roberto Rodriguez ...  
🔗 [threathunterplaybook.com](https://threathunterplaybook.com)



 64

 134





<https://twitter.com/HunterPlaybook/status/1301207718355759107>

# Repeatable? Practical? SIEM Agnostic?



Launch Binder



Colab



Live Code

Contents

## Metadata

Technical Description

Hypothesis

Analytics

Detection Blindspots

Hunter Notes

Hunt Output

References

## Metadata

id WIN-200902020333

author Roberto Rodriguez @Cyb3rWard0g

creation date 2020/09/02

platform Windows

playbook link

# Repeatable? Practical? SIEM Agnostic?



Starting repository: OTRF/ThreatHunter-Playbook/master

If a repository takes a long time to launch, it is usually because Binder needs  
to create the environment for the first time.

Build logs

hide

```
Found built image, launching...
Launching server...
```

# Repeatable? Practical? SIEM Agnostic?

The screenshot shows a Jupyter Notebook interface on a browser. The title bar indicates the notebook is titled "jupyter WIN-200902020333 (autosaved)" and is running on "PySpark\_Python3". The top menu includes File, Edit, View, Insert, Cell, Kernel, Help, and various toolbar icons. The main content area has a section titled "Remote WMI ActiveScriptEventConsumers" with a "Metadata" table:

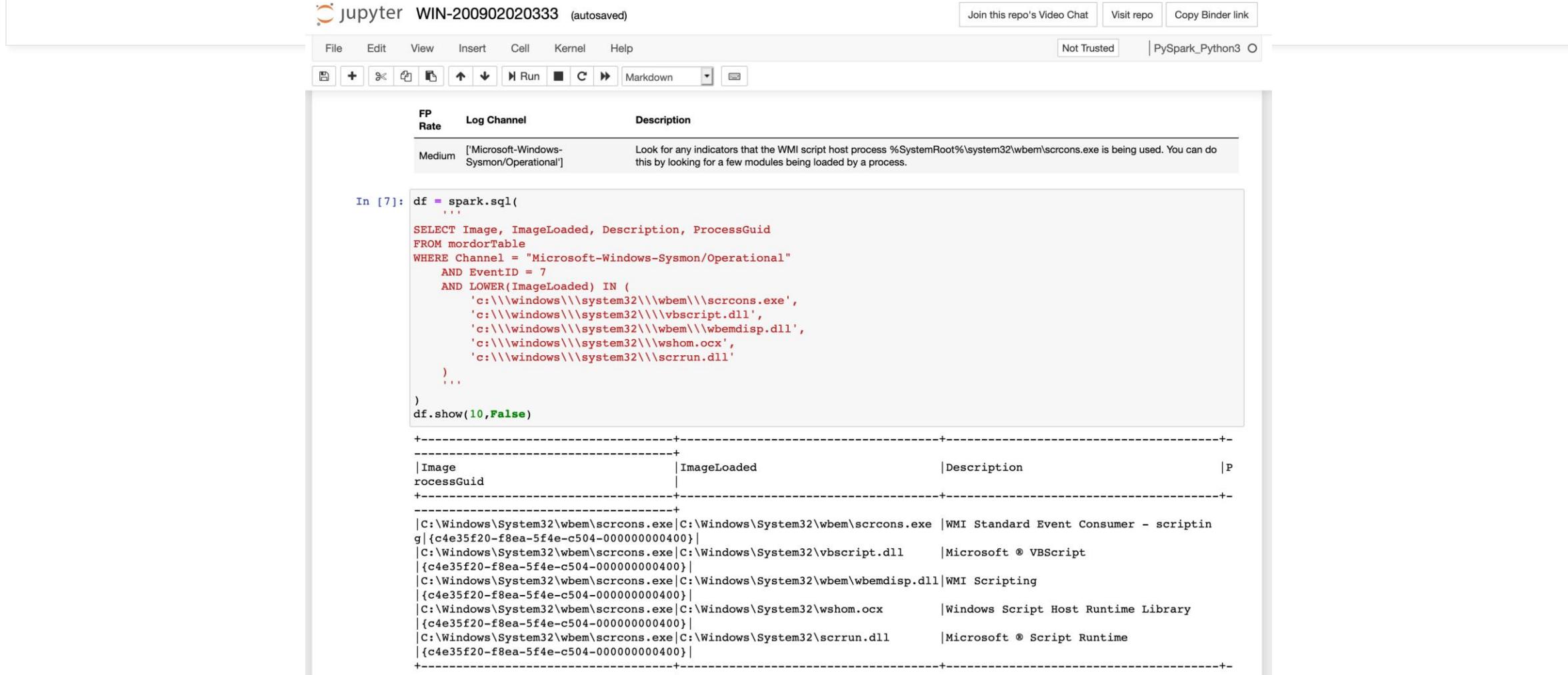
id	WIN-200902020333
author	Roberto Rodriguez @Cyb3rWard0g
creation date	2020/09/02
platform	Windows
playbook link	

Below the table is a "Technical Description" section:

Threat actors can achieve remote code execution by using WMI event subscriptions. Normally, a permanent WMI event subscription is designed to persist and respond to certain events. According to [Matt Graeber](#), if an attacker wanted to execute a single payload however, the respective event consumer would just need to delete its corresponding event filter, consumer, and filter to consumer binding. The advantage of this technique is that the payload runs as SYSTEM, and it avoids having a payload be displayed in plaintext in the presence of command line auditing.

One of the components of an Event subscription is the event consumer. It is basically the main action that gets executed when a filter triggers (i.e. monitor for authentication events. if one occurs. trigger the consumer).

# Repeatable? Practical? SIEM Agnostic?



The screenshot shows a Jupyter Notebook interface with the title "jupyter WIN-200902020333 (autosaved)". The notebook has tabs for File, Edit, View, Insert, Cell, Kernel, and Help. A toolbar below includes icons for file operations like Open, Save, and Run, along with Run, Kernel, and Help buttons. The status bar indicates "Not Trusted" and "PySpark\_Python3".

A log entry is displayed in a table:

FP Rate	Log Channel	Description
Medium	['Microsoft-Windows-Sysmon/Operational']	Look for any indicators that the WMI script host process %SystemRoot%\system32\wbem\scrcons.exe is being used. You can do this by looking for a few modules being loaded by a process.

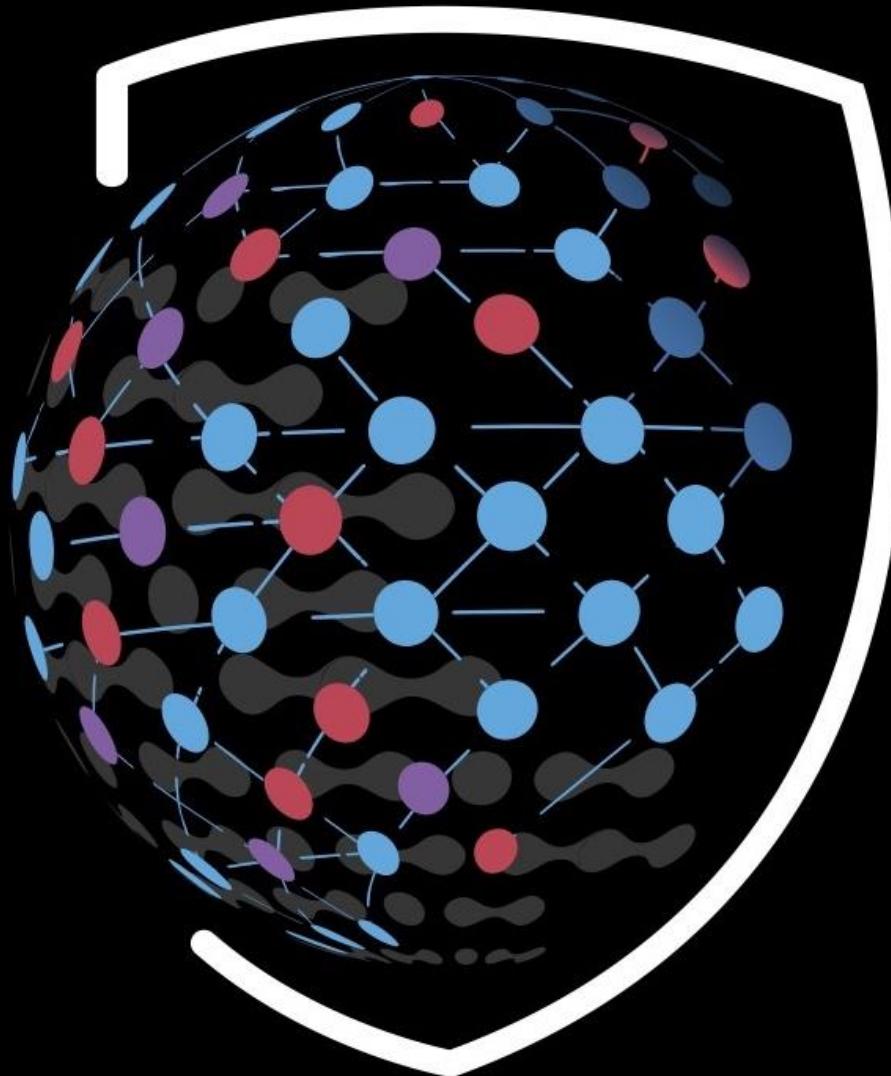
In [7]:

```
df = spark.sql(  
    """  
    SELECT Image, ImageLoaded, Description, ProcessGuid  
    FROM mordorTable  
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND EventID = 7  
        AND LOWER(ImageLoaded) IN (  
            'c:\\\\windows\\\\system32\\\\wbem\\\\scrcons.exe',  
            'c:\\\\windows\\\\system32\\\\vbscript.dll',  
            'c:\\\\windows\\\\system32\\\\wbem\\\\wbemdisp.dll',  
            'c:\\\\windows\\\\system32\\\\wshom.ocx',  
            'c:\\\\windows\\\\system32\\\\scrrun.dll'  
        )  
    )  
df.show(10, False)
```

The output of the query is a DataFrame:

Image	ImageLoaded	Description	P
Image	ImageLoaded	Description	P
rocessGuid			
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\wbem\scrcons.exe  WMI Standard Event Consumer - scriptin			
g {c4e35f20-f8ea-5f4e-c504-000000000400}			
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\vbscript.dll  Microsoft ® VBScript			
{c4e35f20-f8ea-5f4e-c504-000000000400}			
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\wbem\wbemdisp.dll WMI Scripting			
{c4e35f20-f8ea-5f4e-c504-000000000400}			
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\wshom.ocx  Windows Script Host Runtime Library			
{c4e35f20-f8ea-5f4e-c504-000000000400}			
C:\Windows\System32\wbem\scrcons.exe C:\Windows\System32\scrrun.dll  Microsoft ® Script Runtime			
{c4e35f20-f8ea-5f4e-c504-000000000400}			

**Thank you! Gracias!**



# OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY

# Sweet slide citations!



NASA Image and Video Library; <https://images.nasa.gov/>



# OSS Hunting and Adversarial Simulation

What are we doing here?



Pre-Show Banter



Panelist Discussion: OSS Community Problems



Project Spotlight: Open Threat Research



?? Post Show Show Banter ??