

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



~~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-Monetize

- Late night
- Duplicat
- Is it gettin

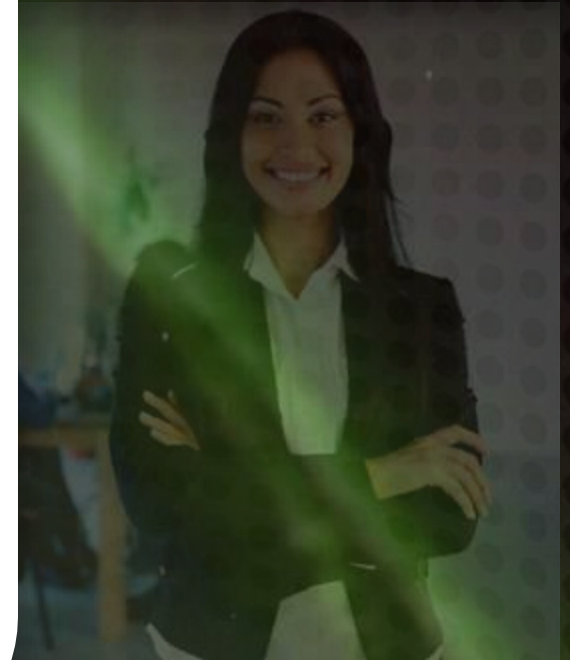
Re-Investing O

- WWHF Tr
- Commer

Why I Hate Threat Intel

BLACK HILLS
© Black Hills Information Security | @BHInfoSecurity

4:07 / 1:15:05 • Threat Intel: A Useless Rant



~~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)

(
R
F

Marcello @oyt20130418 · 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 opt...



GitHub Gist

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

© Black Hills
@BHInfoSec

Source Community is Tired

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/smal...

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

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



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

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

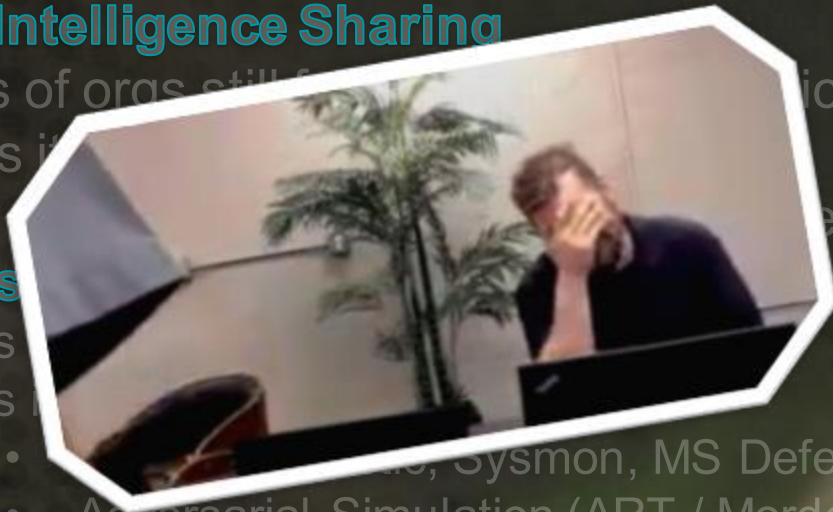


Threat Intelligence Sharing

- Lots of orgs still...
- Is it...
- ...growing (ar...

Hackers

- Is...
- Is...
- ...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

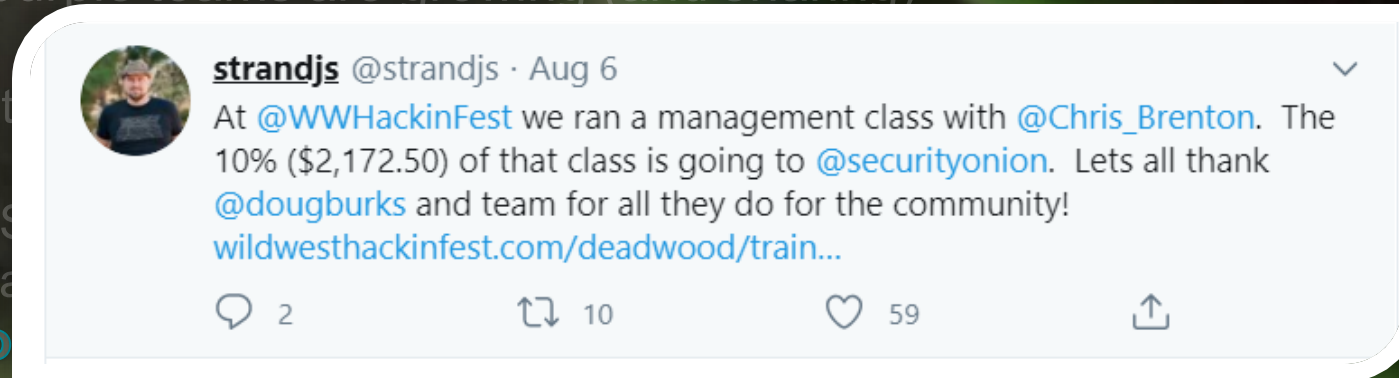
- Is defenders fatigue a thing?
- Is it getting better?
 - Yes, see: Elastic, S
 - Adversarial Simula

(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



~~Executive Problem Statement~~ OSS Community ^ Discussion



Audience Questions



OSS Hunting and Adversarial Simulation

What are we doing here?



Pre-Show Banter



Panelist Discussion: OSS Community Problems



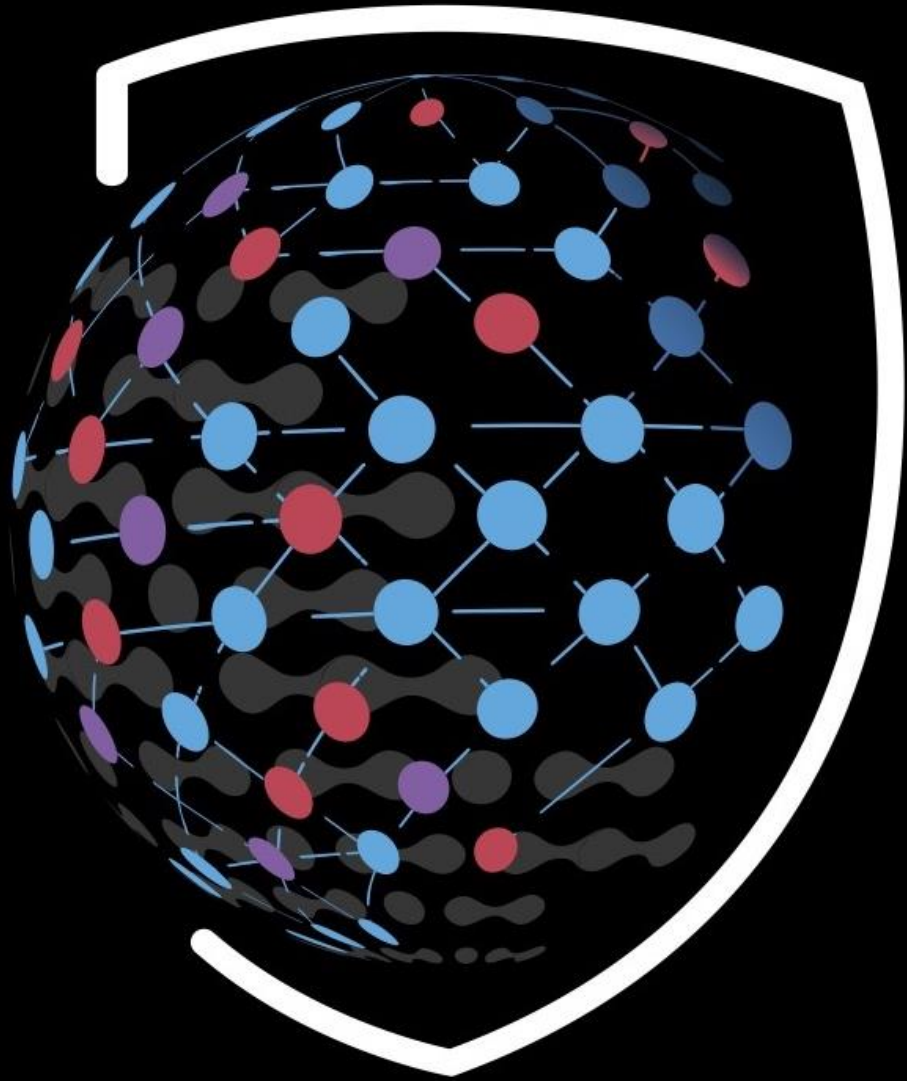
Project Spotlight: Open Threat Research

Mordor & Mordor Datasets

Intermission



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



OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY

Roberto Rodriguez

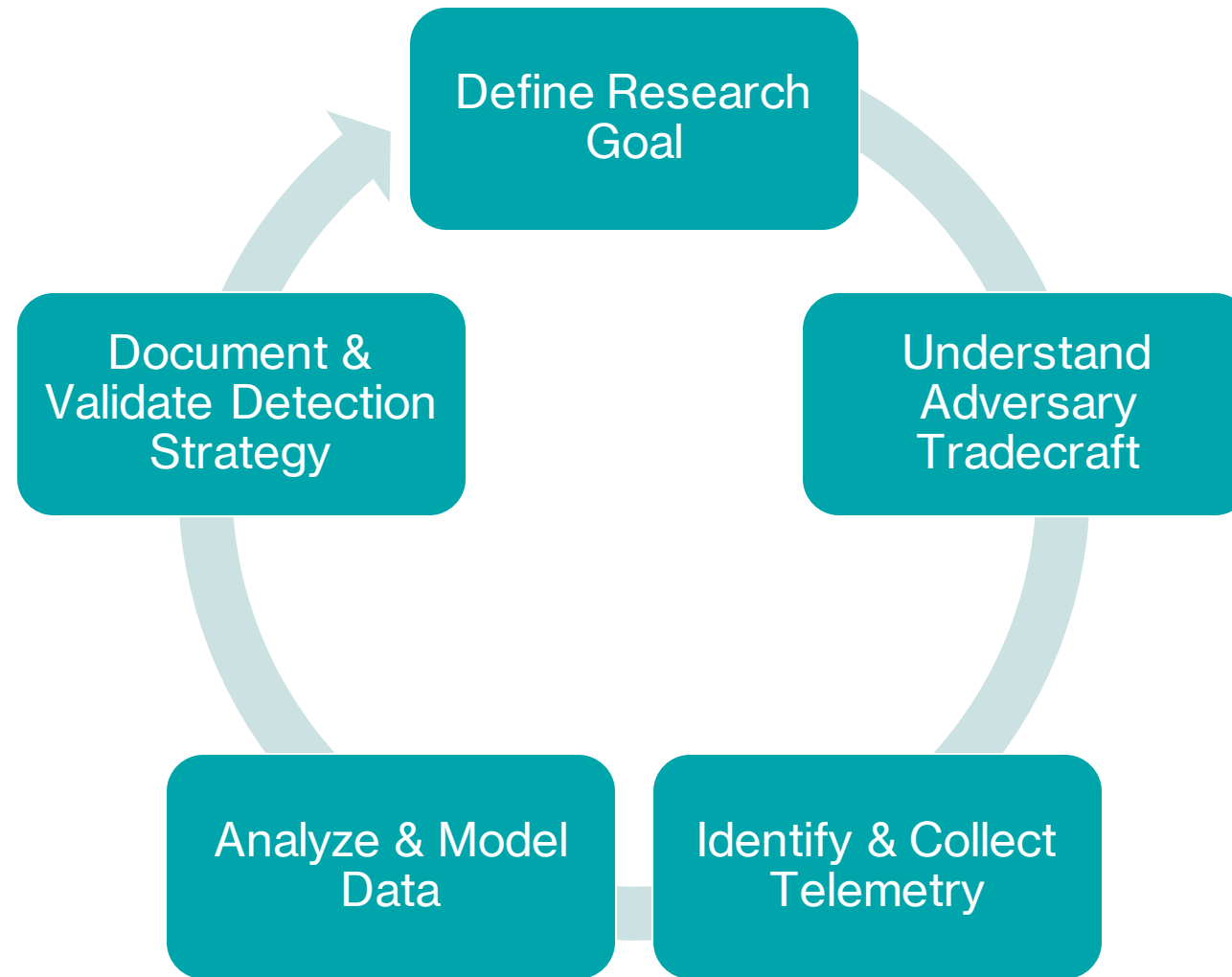
@Cyb3rWard0g

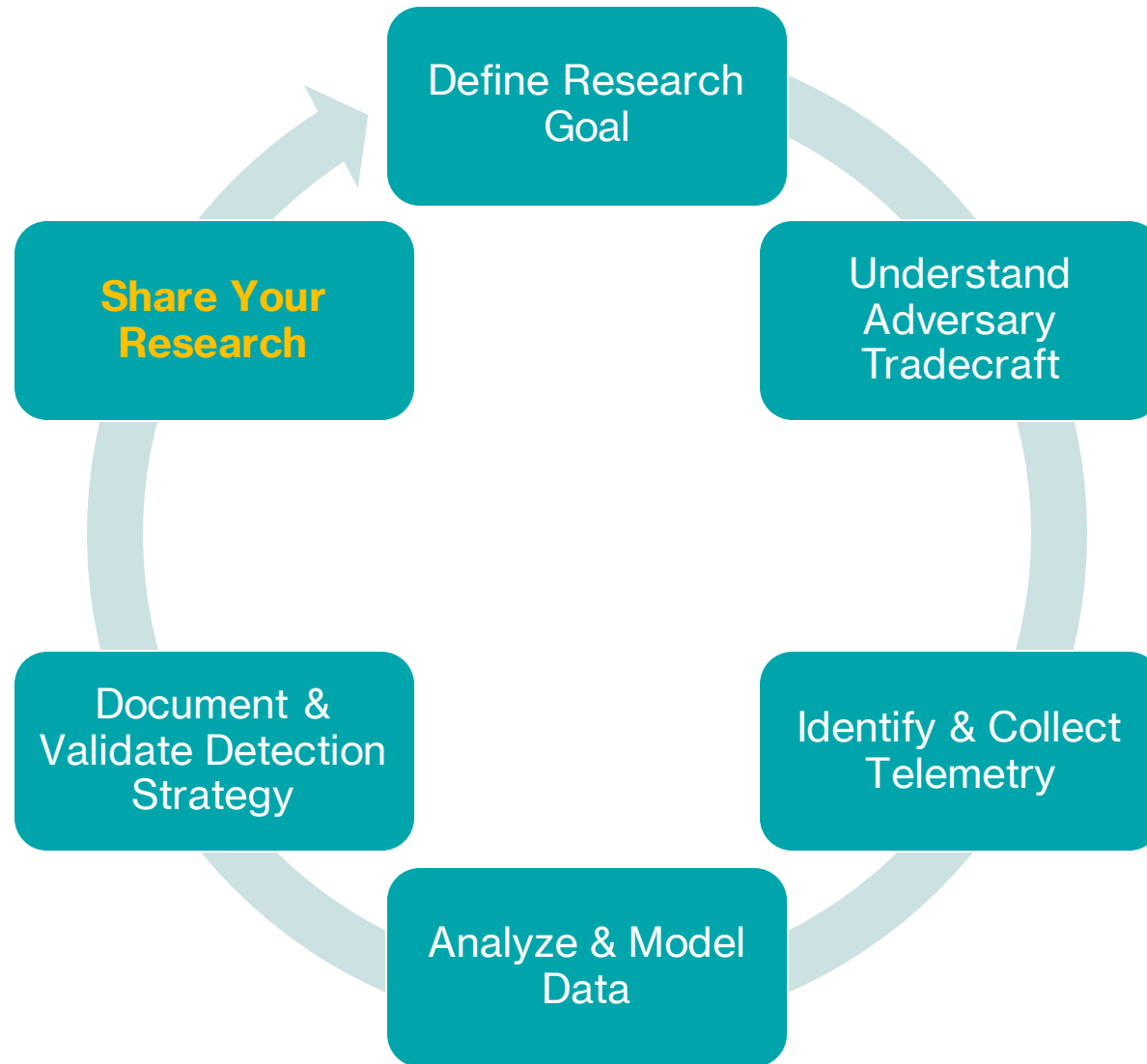
- Microsoft Threat Intelligence Center (MSTIC) R&D
- Open Source ♥
 - Threat Hunter Playbook [@HunterPlaybook](#)
 - Mordor [@Mordor_Project](#)
 - OSSEM [@OSSEM_Project](#)
 - Blacksmith & more..
- Open Threat Research Founder

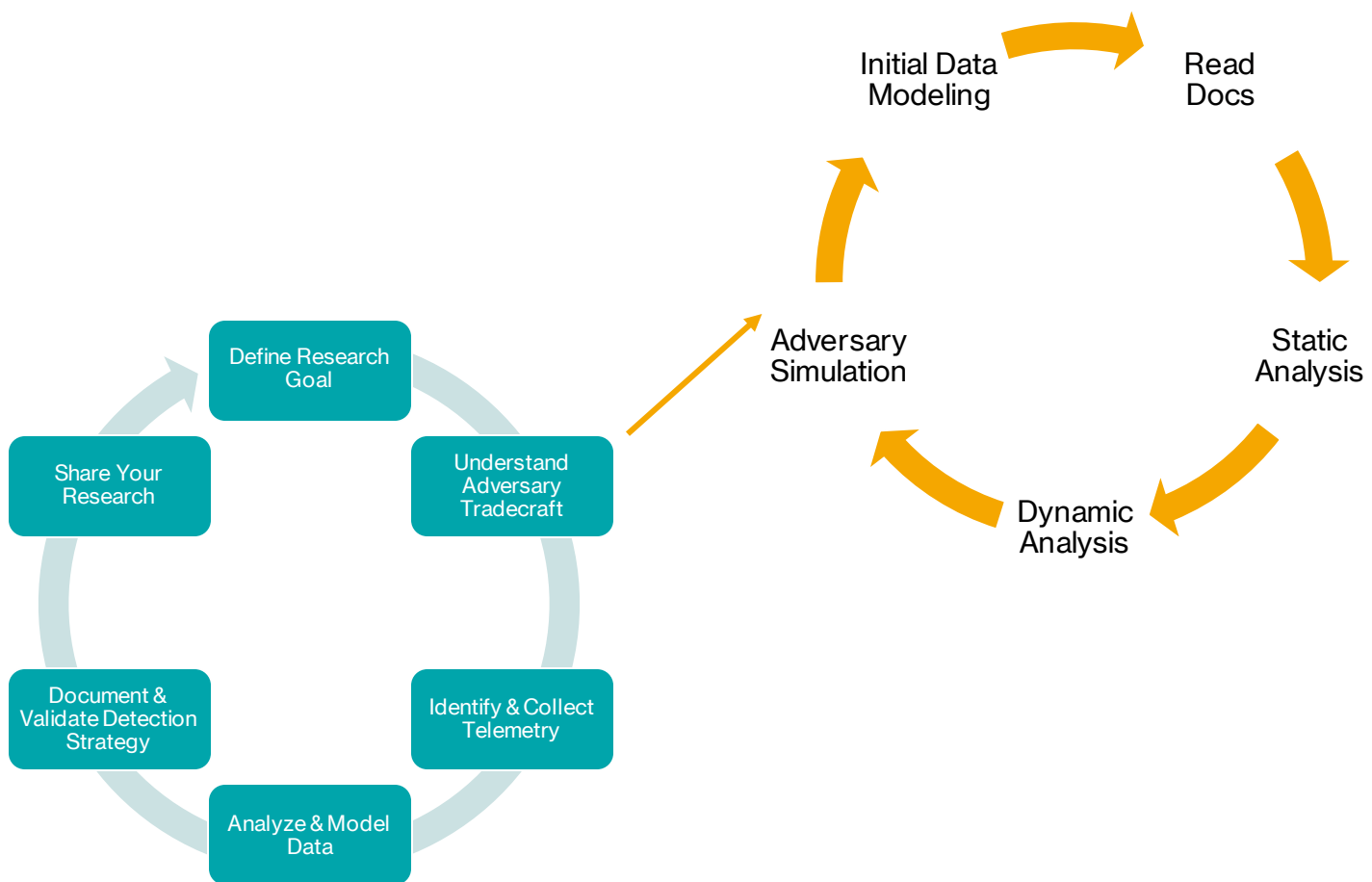


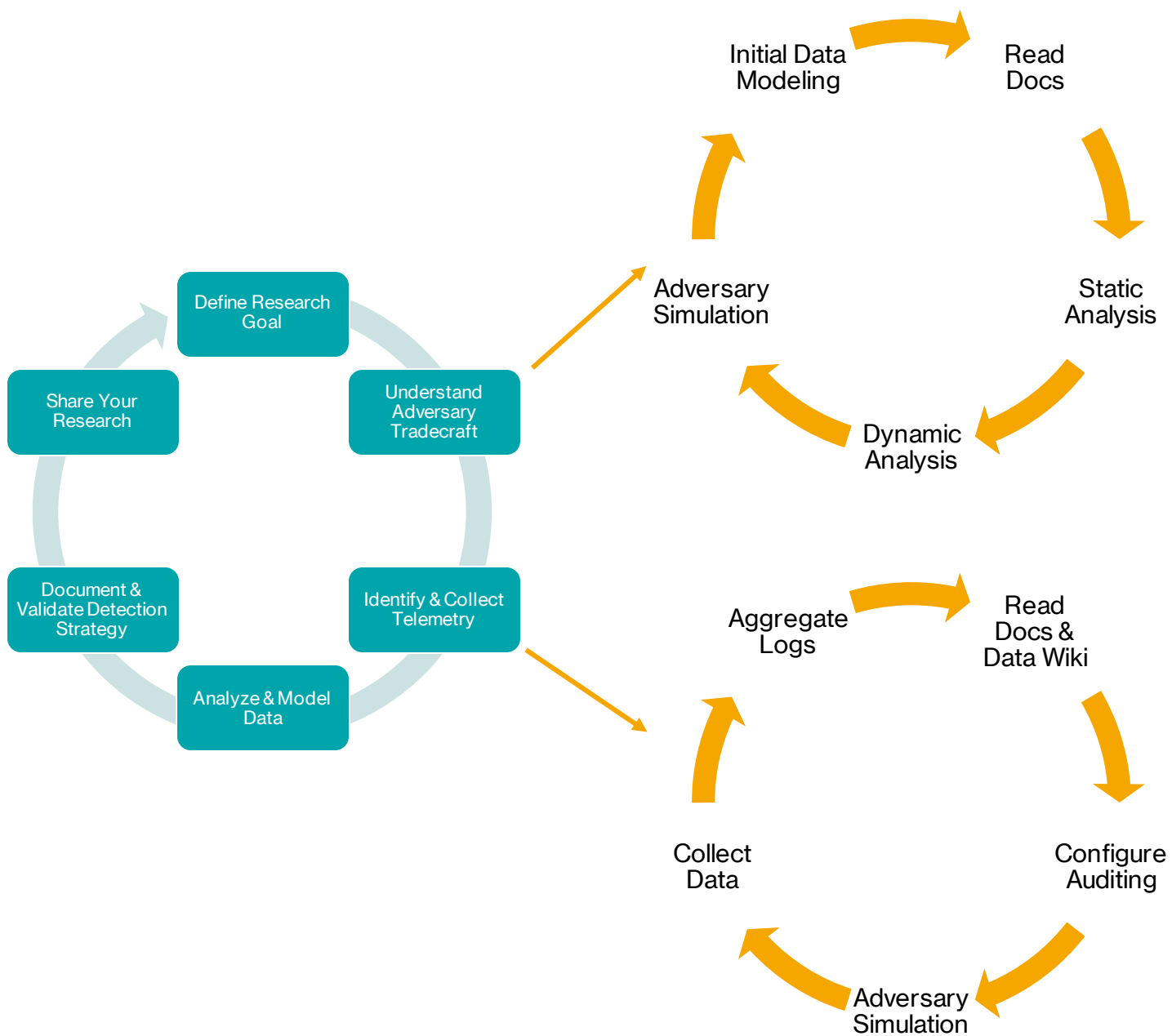
Threat Research

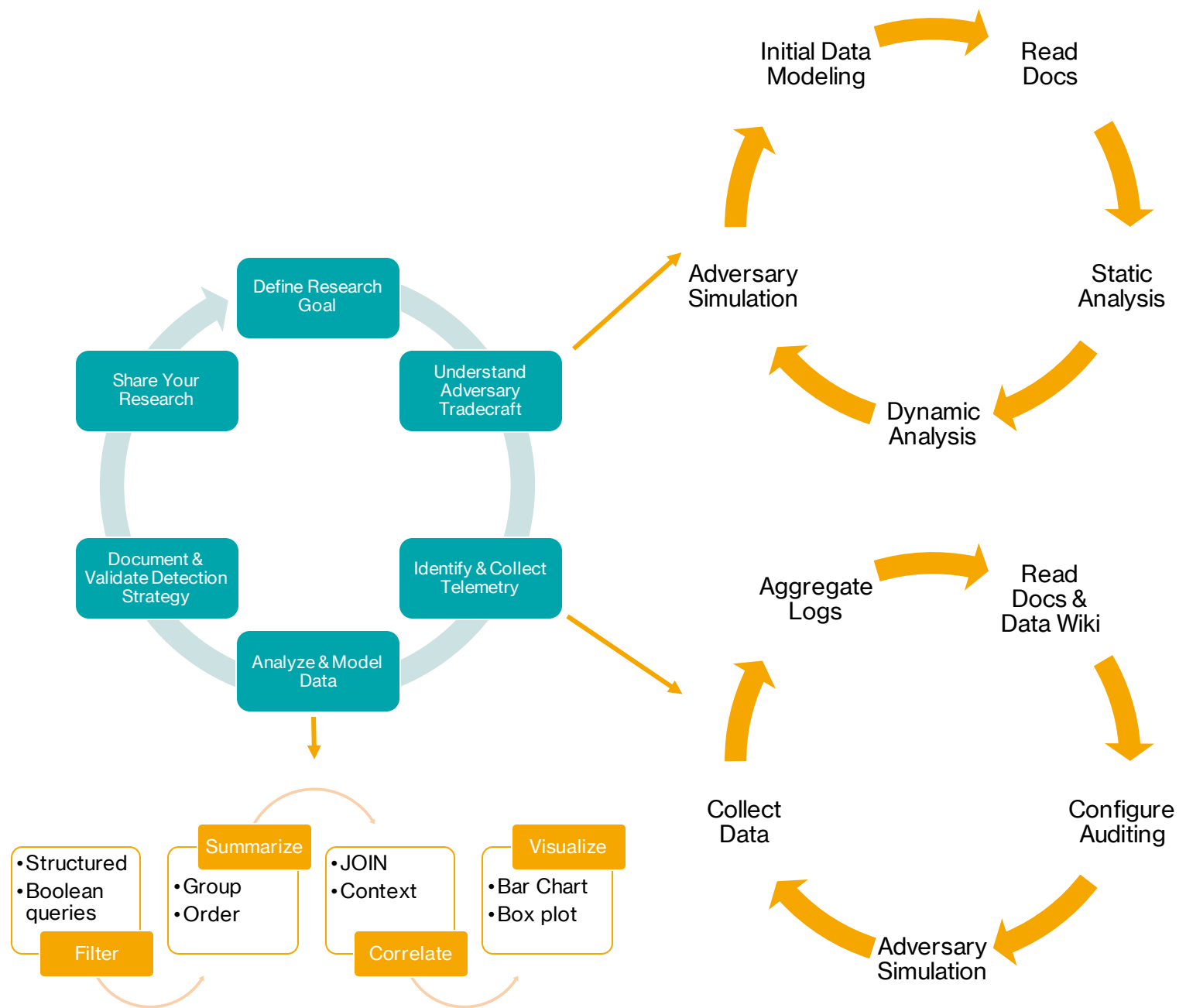


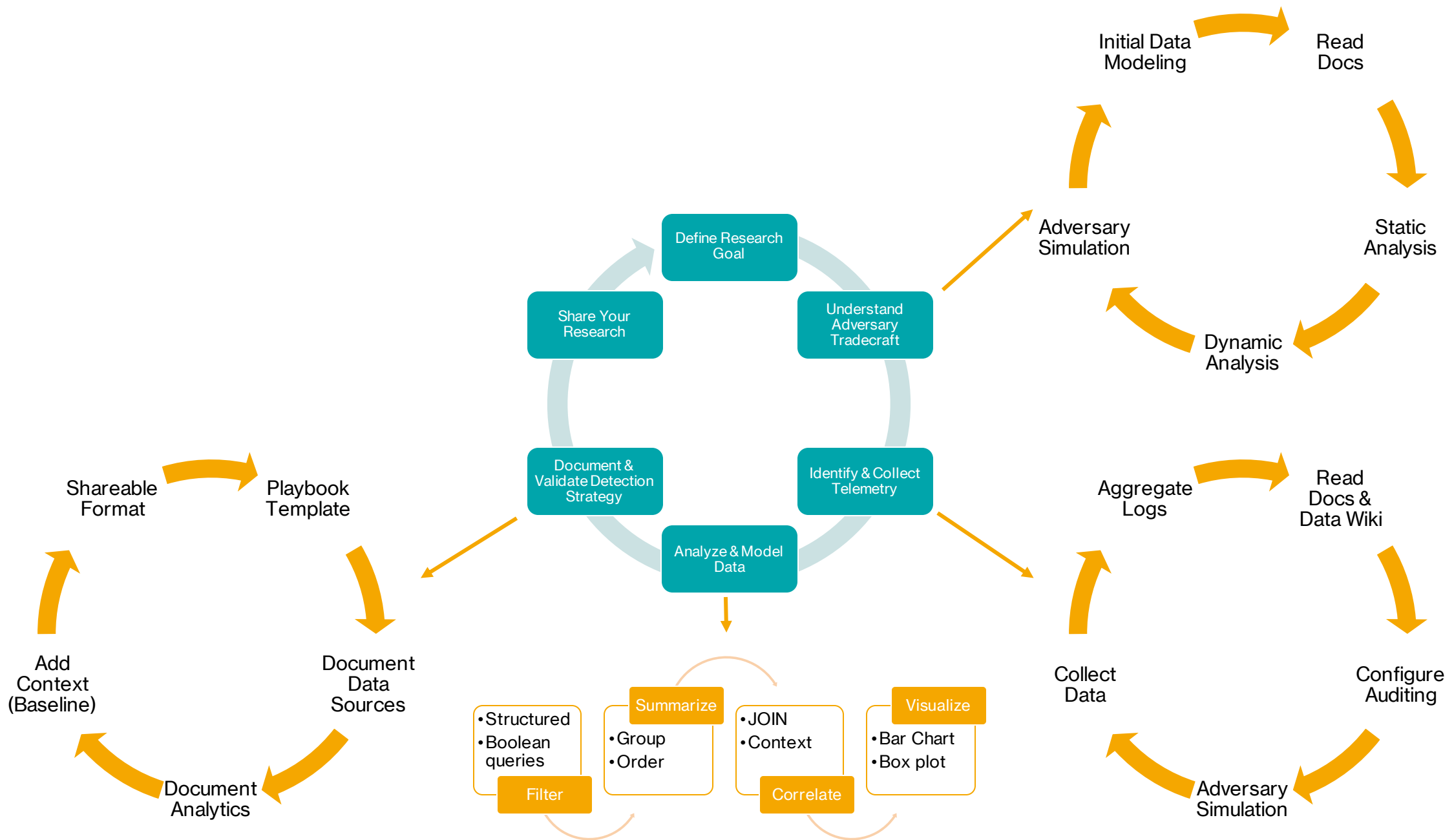


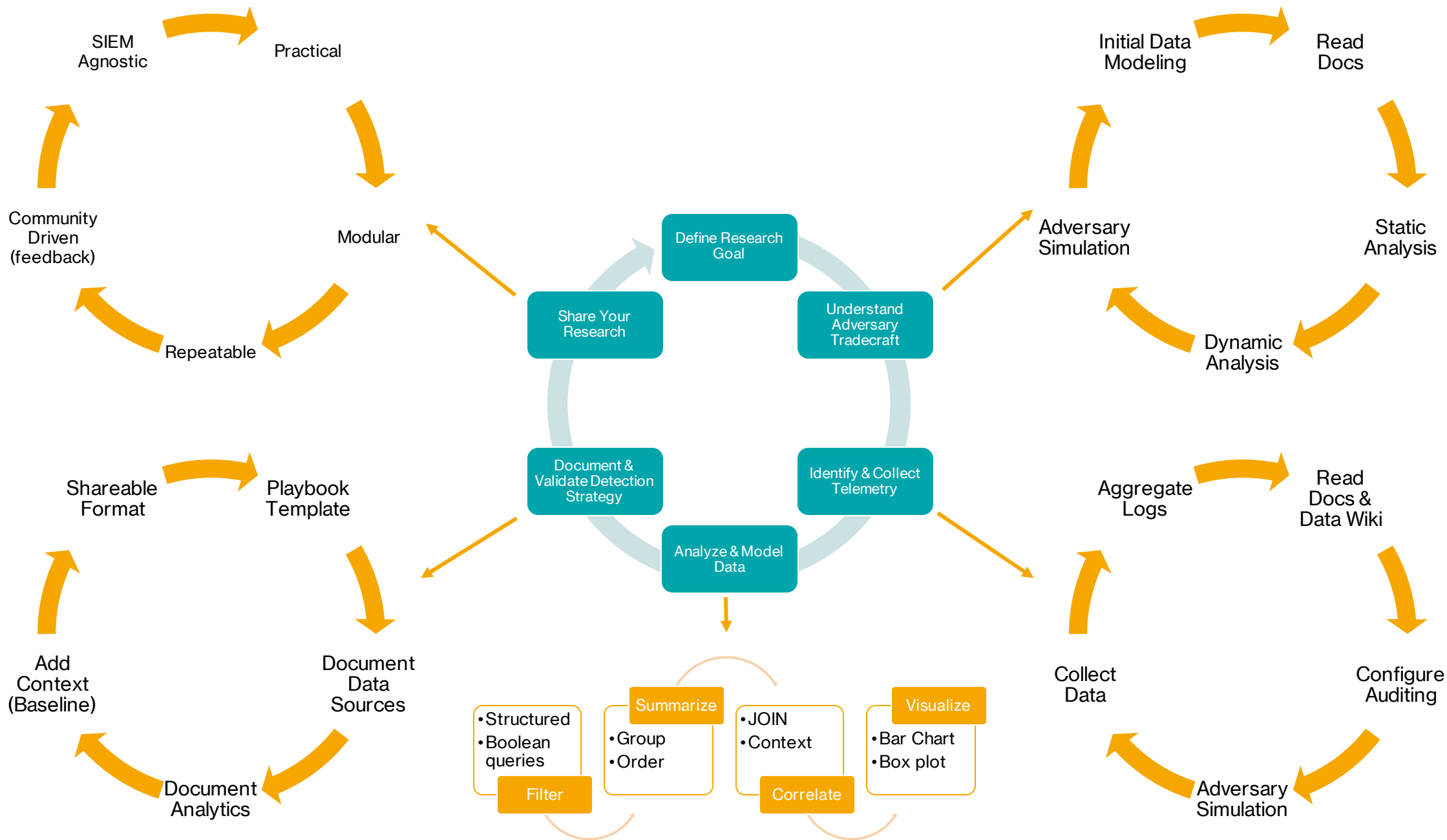


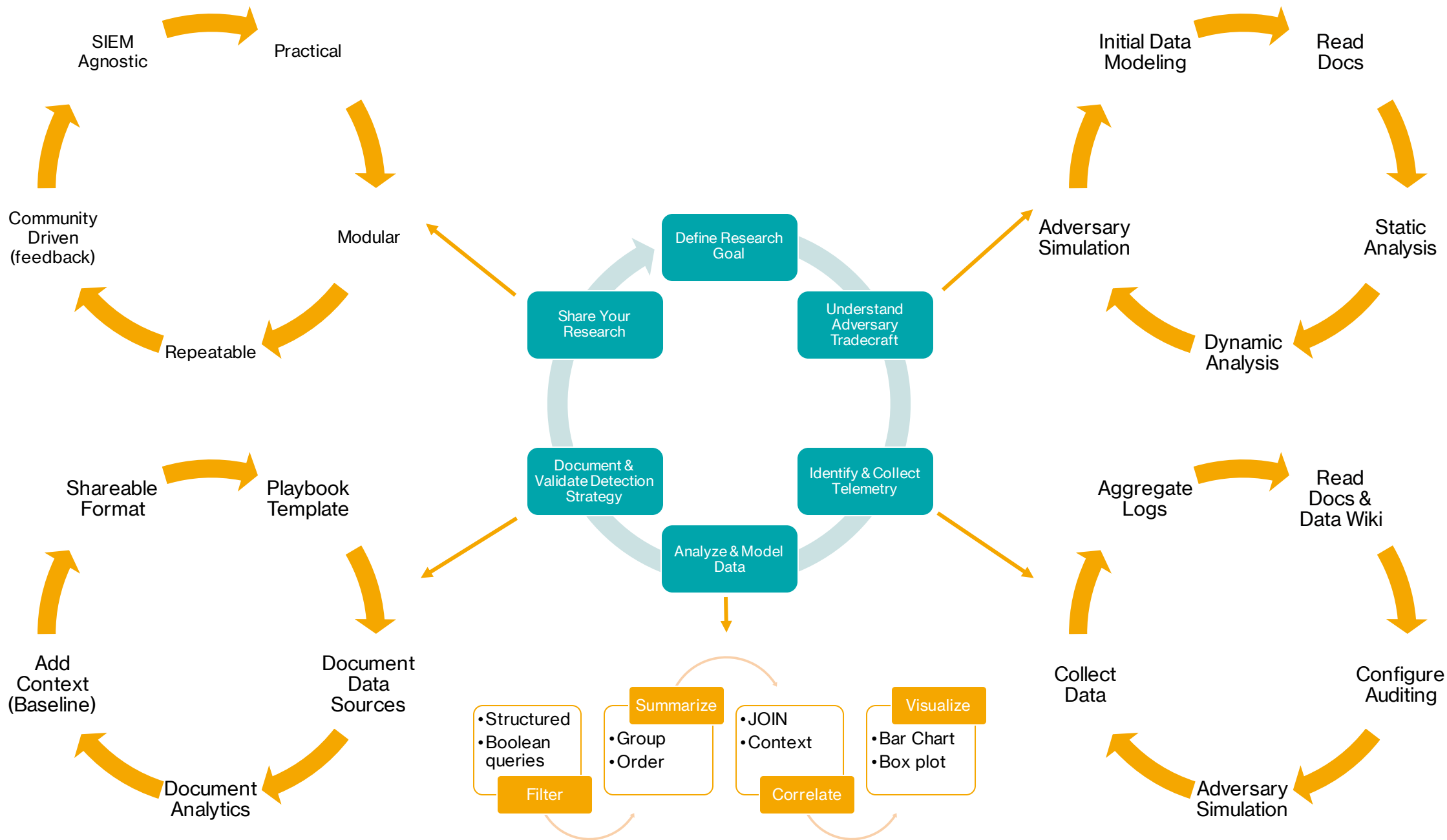




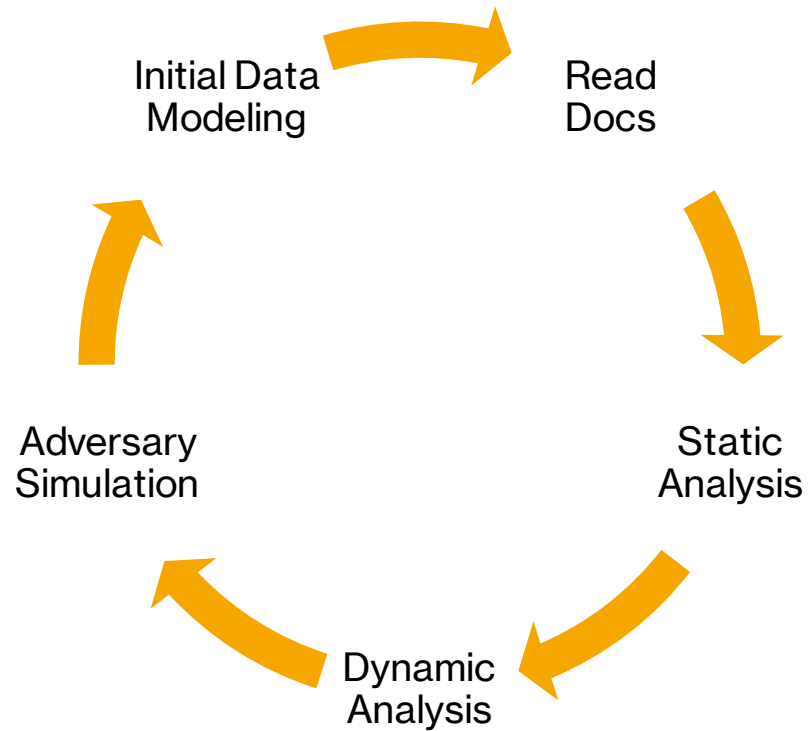




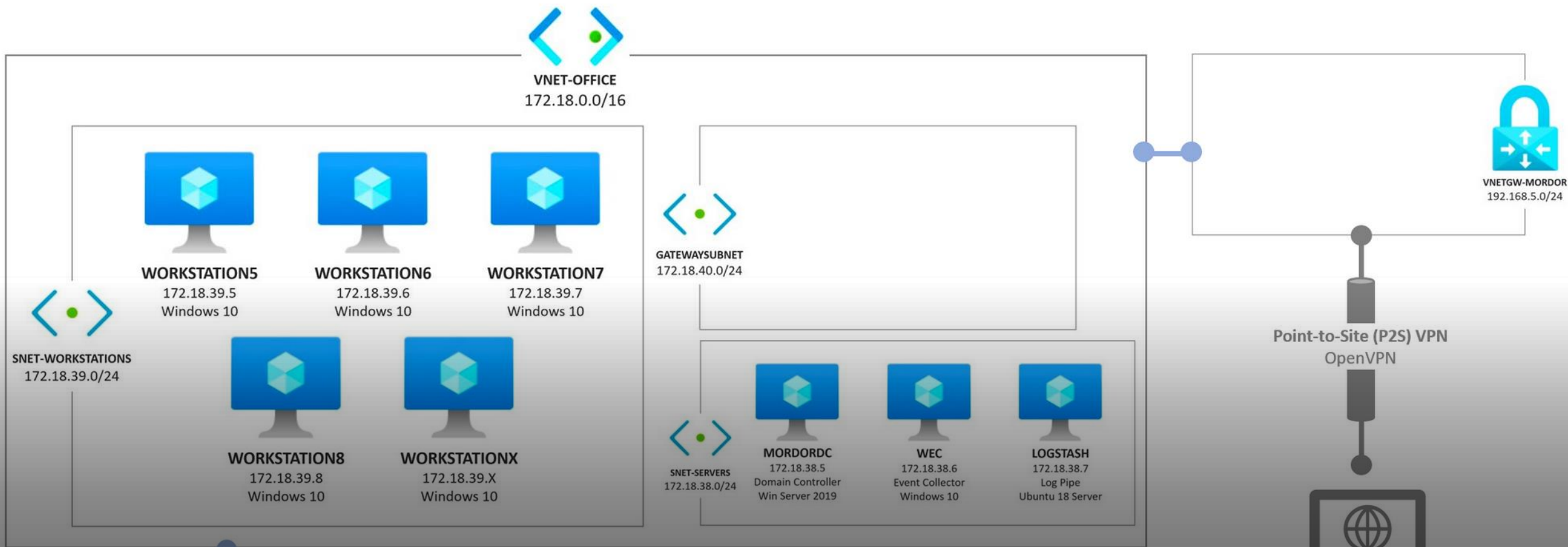




Understand Adversary Tradecraft



- Read Docs
- Mordor Labs Project
- Mordor Project

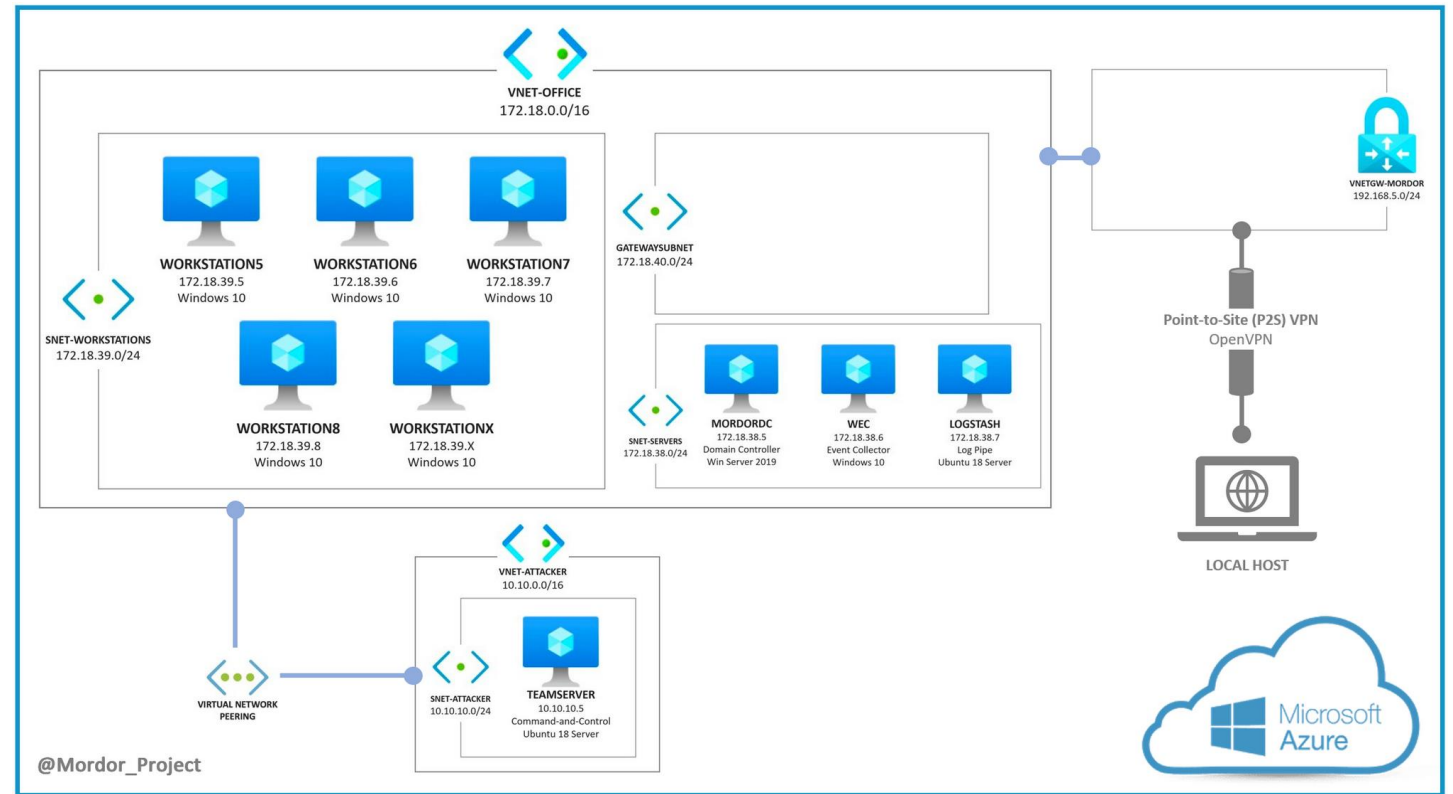


Mordor Labs

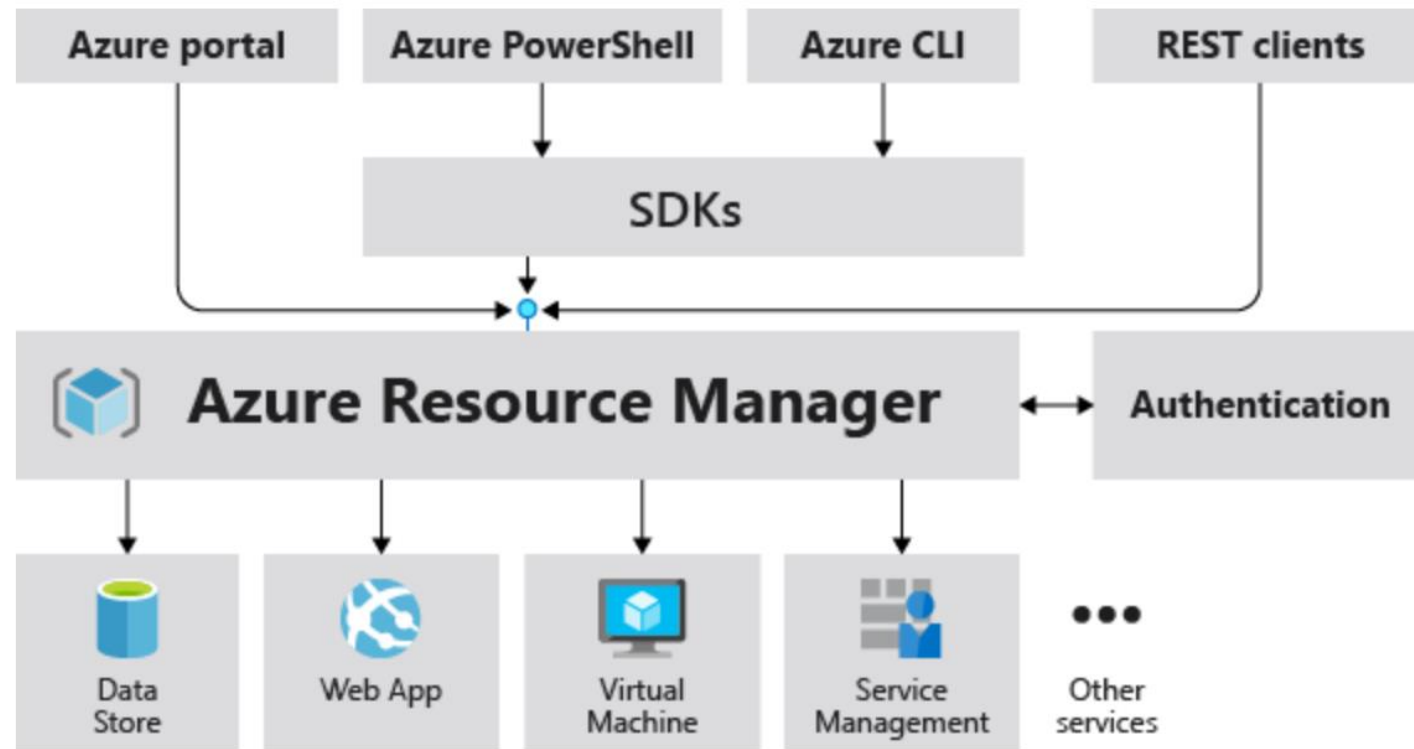
Mordor Labs

- 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

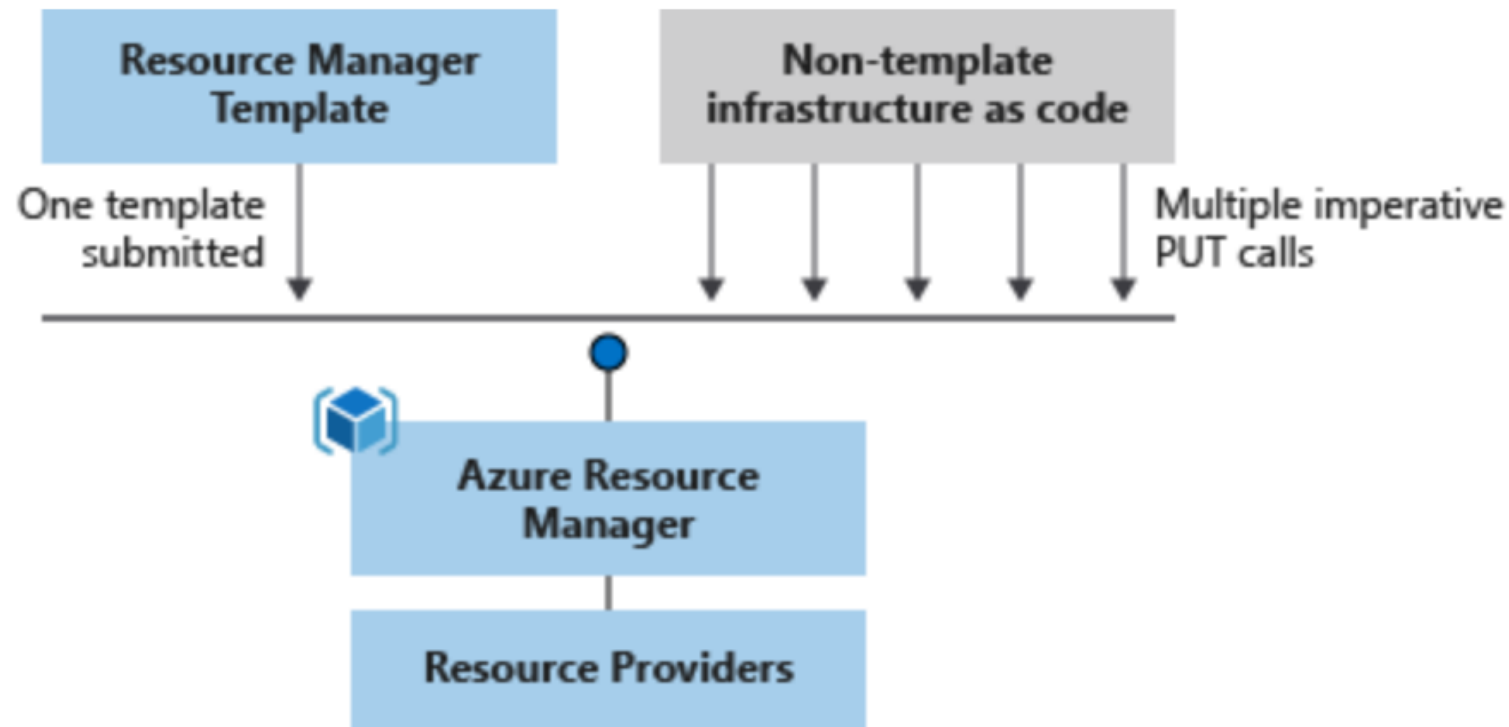
Windows: The Shire



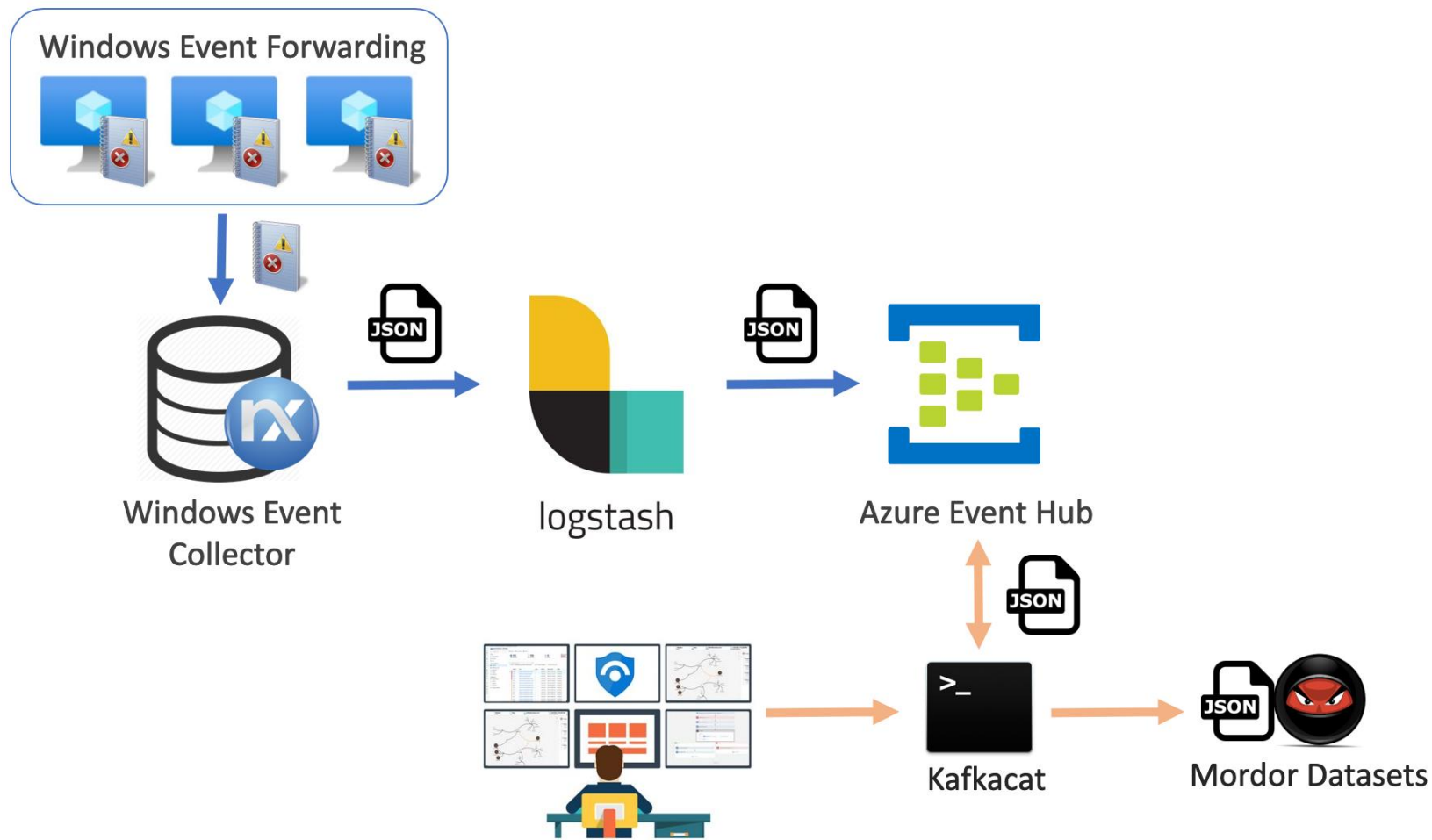
Azure Resource Manager Service



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

master Blacksmith / resources / scripts / powershell / auditing /



Cyb3rWard0g Updated WEF and Prepare box script

```

63 $ServiceRules = @"
64 service;addition
65 "IKEEXT";"(AU;SAFA;RPWPTCCLC;;;WD)"
66 "SessionEnv";"S:(AU;SAFA;RPWPTCCLC;;;WD)"
67 "scmanager";"(AU;SAFA;GA;;;NU)"
68 "@
69
70 $ServiceRules | ConvertFrom-Csv -Delimiter ';' | ForEach-Object {
71     if(Get-Service $service){
72         Write-Host "[+] Processing " $_.service
73         # Get Sddl
74         $sddl = (& $env:SystemRoot\System32\sc.exe sdshow $_.service | Out-String).Trim()
75         # Define new Sddl
76         $newSddl = ('{0}{1}' -f $sddl, $_.addition).Trim()
77         # Update Sddl
78         write-host " [>] Updating SDDL.."
79         & $env:SystemRoot\System32\sc.exe sdset $_.service "$newSddl"
80     }
81 }













```

Windows Event Auditing

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

master Blacksmith / resources / configs / wef / subscriptions /

Cyb3rWar

..

bits-client.

directory-s

dns-client.

firewall-ad

powershell

powershell

security.xr

sysmon.xr

system.xml

task-sched

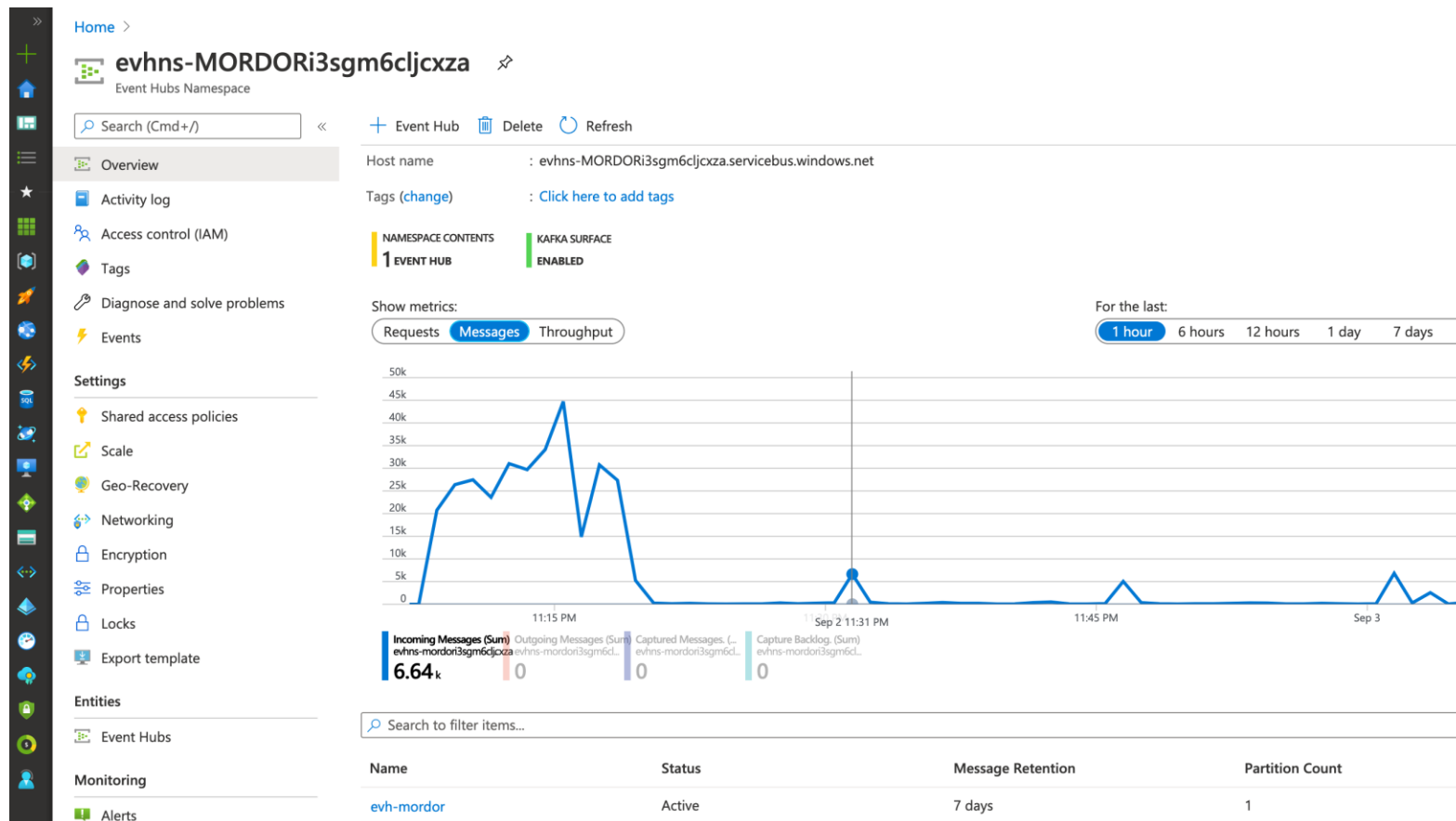
terminal-se

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>0:NSG:BAD:P(A;;GA;;;DC)(A;;GA;;;DD)S:</AllowedSourceDomainComputers>
</Subscription>
```

WEF Subscriptions

Azure Event Hubs



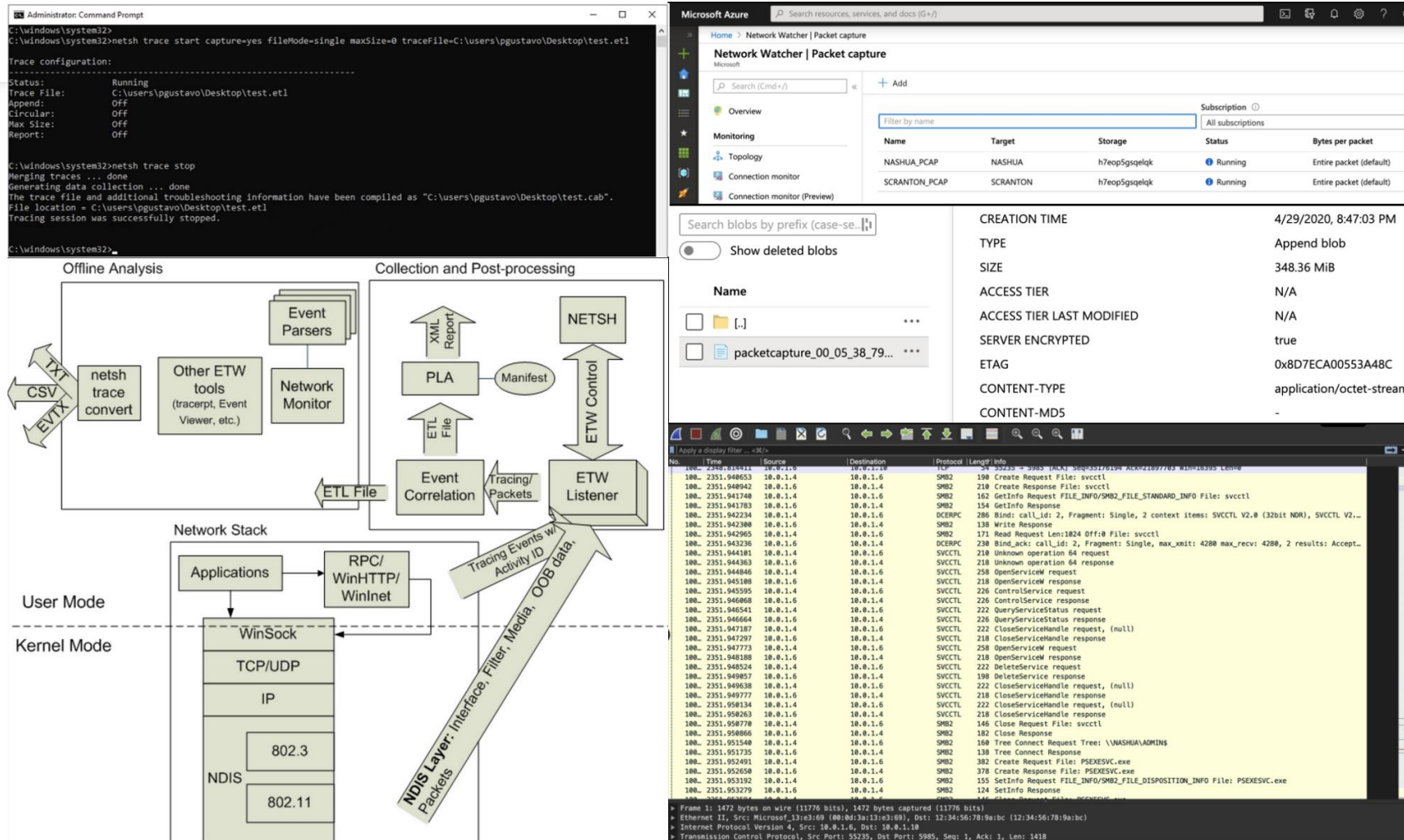
Azure Event Hubs + Kafkacat

- **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
```


What about Network Telemetry?





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

BITS Jobs (0/7)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery (0/7)	Internal Network Discovery (0/7)
Boot or Logon Autostart Execution (1/11)	Boot or Logon Autostart Execution (1/11)	BITS Jobs (0/7)	Exploitation for Credential Access (0/3)	Score: 1	Automated Collection (0/7)
Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information (0/1)	Forced Authentication (0/1)	Browser Bookmark Discovery (0/3)	Clipboard Data (0/1)
Browser Extensions (0/5)	Create or Modify System Process (0/4)	Direct Volume Access (0/1)	Input Capture (0/4)	Domain Trust Discovery (0/3)	Data from Information Repositories (0/1)
Compromise Client Software Binary (0/4)	Event Triggered Execution (1/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	File and Directory Discovery (0/3)	Data from Local System (0/1)
Create Account (0/2)	Exploitation for Privilege Escalation (1/2)	Exploitation for Defense Evasion (0/1)	Modify Authentication Process (0/3)	Network Service Scanning (0/3)	Data from Network Shared Drive (0/1)
Create or Modify System Process (0/4)	Group Policy Modification (0/6)	File and Directory Permissions Modification (1/2)	Network Sniffing (0/3)	Network Share Discovery (0/3)	Data from Removable Media (0/2)
Event Triggered Execution (1/15)	Hijack Execution Flow (1/11)	Group Policy Modification (0/6)	OS Credential Dumping (5/8)	Network Sniffing (0/3)	Data Staged (0/2)
External Remote Services (0/3)	Process Injection (2/11)	Hide Artifacts (0/6)	Steal or Forge Kerberos Tickets (0/3)	Password Policy Discovery (0/3)	Email Collection (0/3)
Hijack Execution Flow (0/3)		Hijack Execution Flow (1/11)	Steal Web (0/3)	Peripheral Device Discovery (0/3)	
		Indicator Removal on (0/3)		Permission Groups Discovery (2/2)	
				Process Discovery (0/3)	
				Query Registry (0/3)	

Table View

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

<https://mordordatasets.com/notebooks/small/windows/windows.html>

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



☰ 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

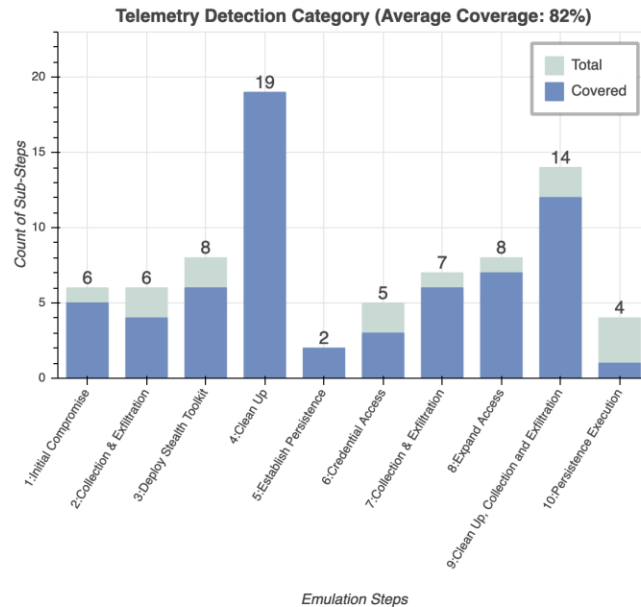
3.B.2. Bypass User Account Control

3.B.3. Commonly Used Port

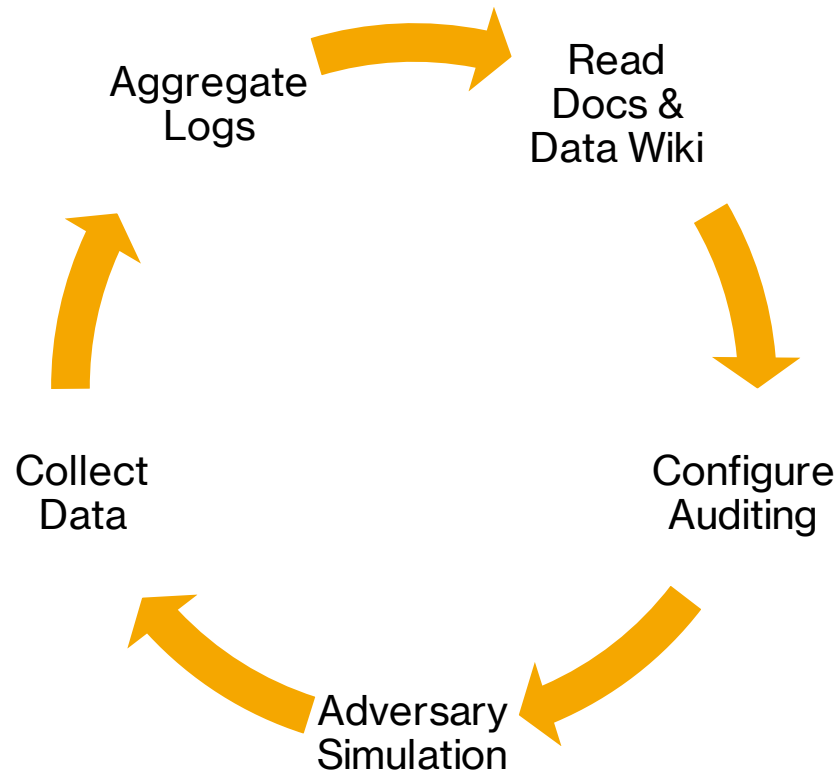
Click to show +

Telemetry Detection Category

BokehJS 2.1.0 successfully loaded.

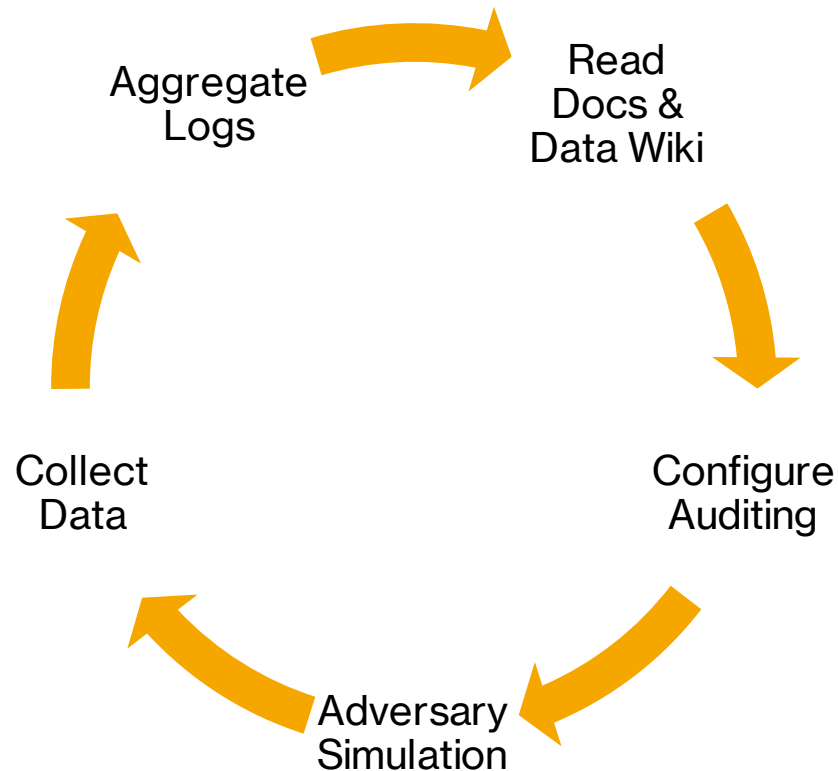


Identify & Collect Telemetry



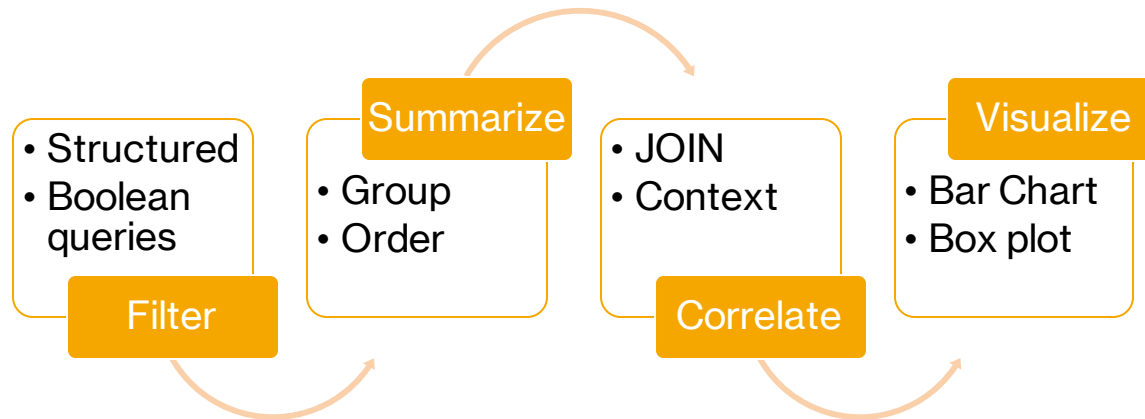
- Read Docs
- Community Data Wiki
- Community Common Data Model

Identify & Collect Telemetry



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

Analyze & Model Data

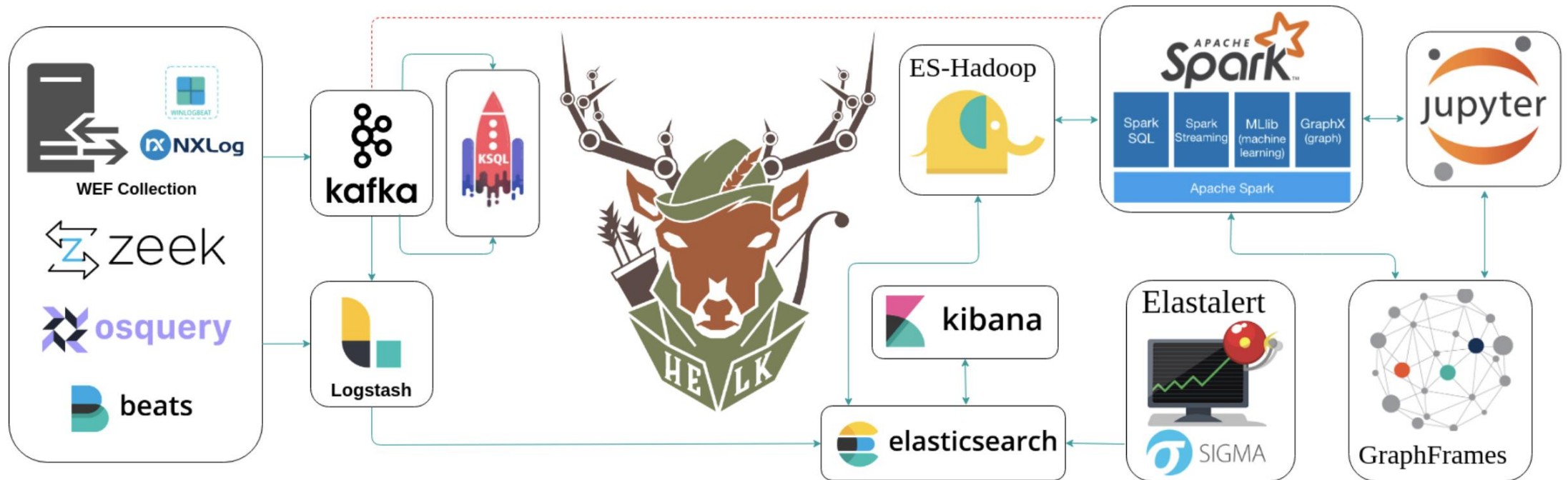


- Transform & Enrich Data
- Initial Data Exploration
- Jupyter Notebooks

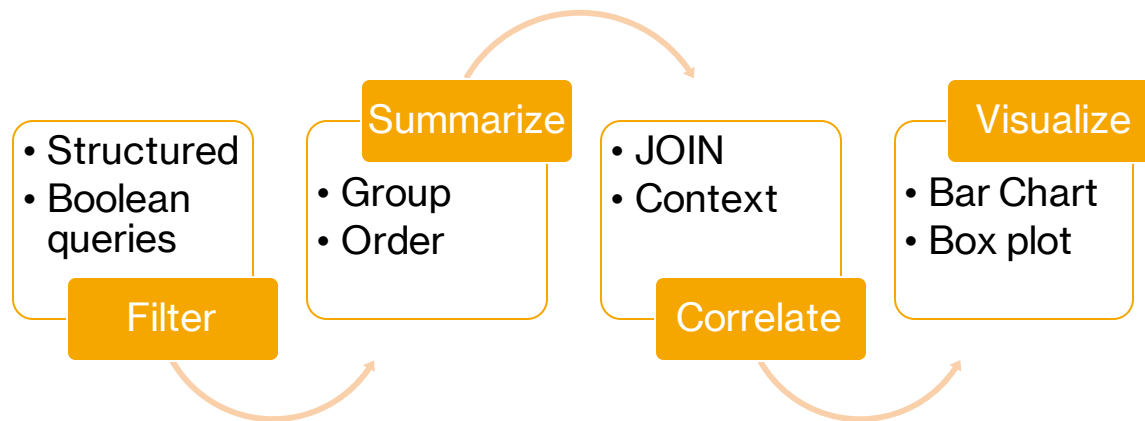
HELK



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
[>>> █
```

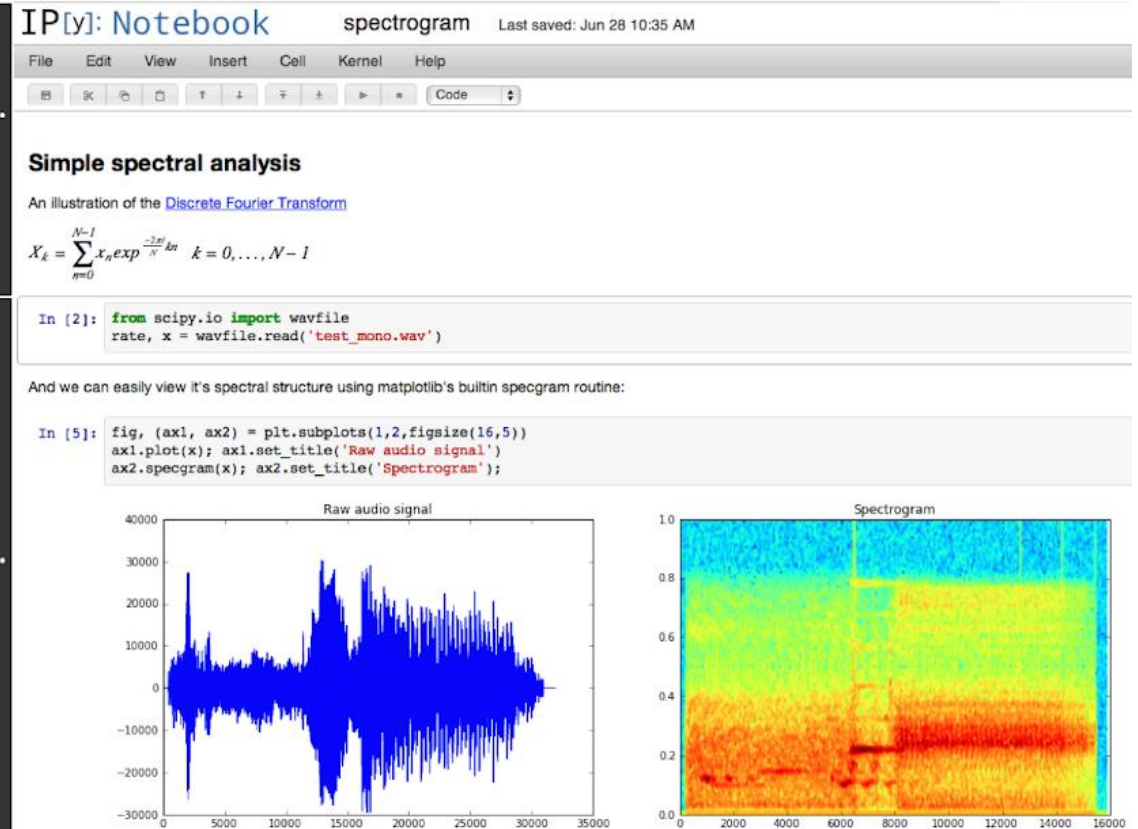
```
[Robertos-MacBook-Pro:GitHub wardog$ ipython
Python 2.7.10 (default, Oct 6 2017, 22:29:07)
Type "copyright", "credits" or "license" for more information.

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.
```

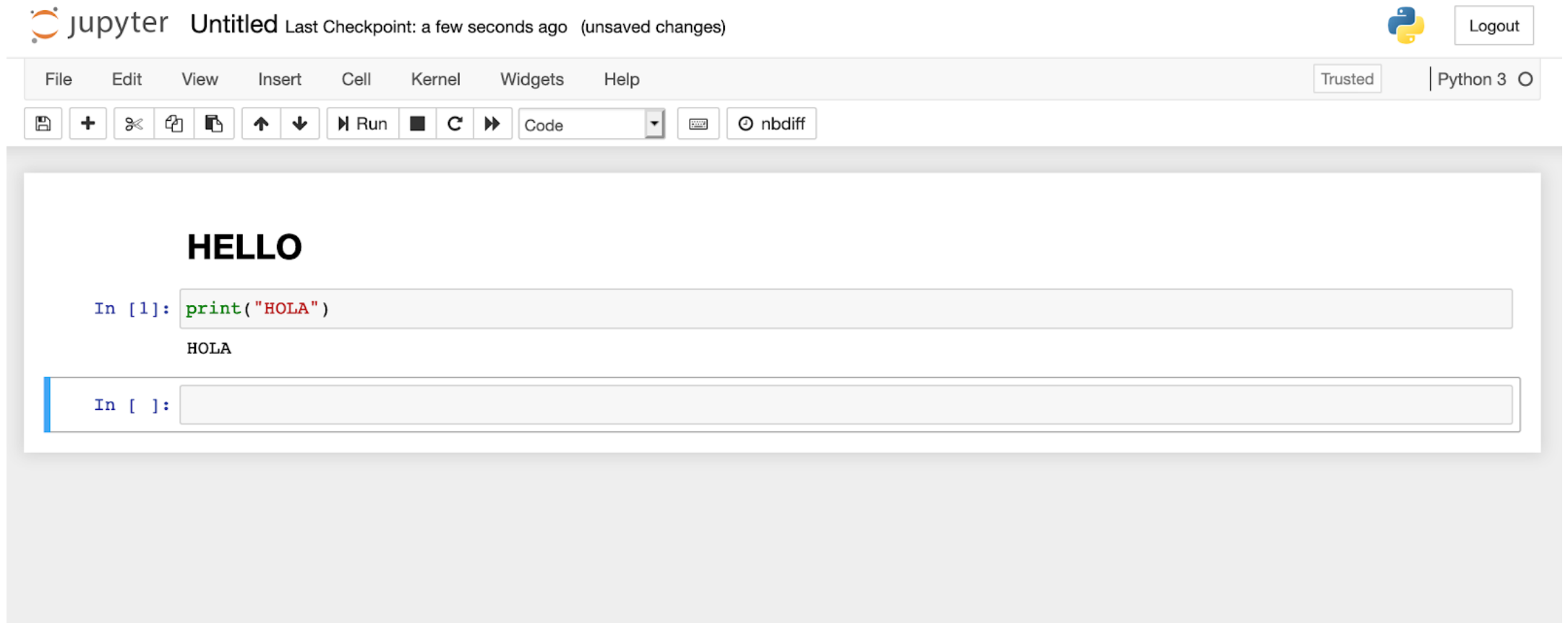
```
[In [1]: print('Hola IPython!!')
Hola IPython!!
```

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

```
In [3]: █
```

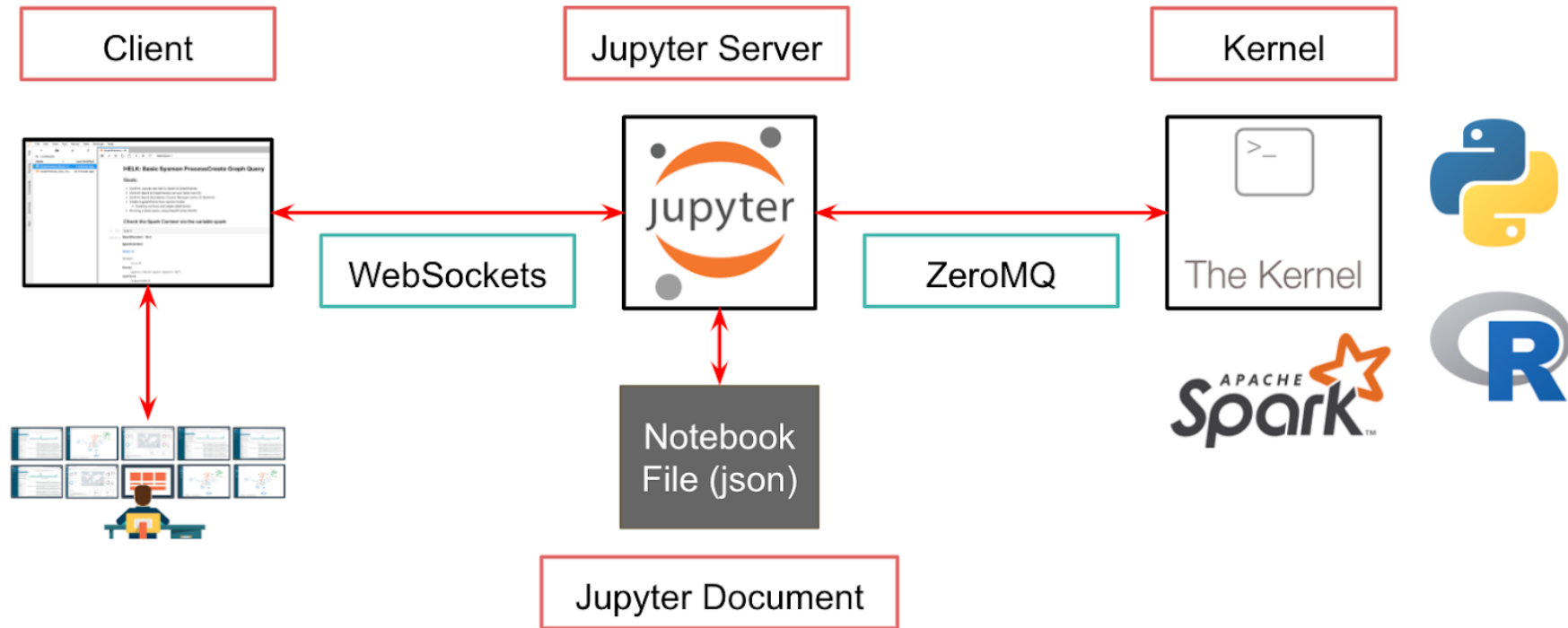


What is a Jupyter Notebook?



The screenshot displays the Jupyter Notebook web interface. At the top, the header shows the Jupyter logo, the text "jupyter", and "Untitled" followed by "Last Checkpoint: a few seconds ago (unsaved changes)". On the right, there is a Python logo and a "Logout" button. Below the header is a menu bar with options: File, Edit, View, Insert, Cell, Kernel, Widgets, and Help. To the right of the menu bar are "Trusted" and "Python 3" indicators. A toolbar below the menu bar contains icons for saving, adding, deleting, and duplicating cells, as well as navigation arrows, a "Run" button, a "Code" dropdown menu, and an "nbdiff" button. The main workspace contains a code cell with the text "HELLO" in large bold letters. Below this, the input prompt "In [1]:" is followed by the code `print("HOLA")` in a light gray box. The output "HOLA" is displayed below the code. At the bottom, there is an empty code cell with the input prompt "In []:".

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 -
CreatRemoteThread

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	RightsRequested
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

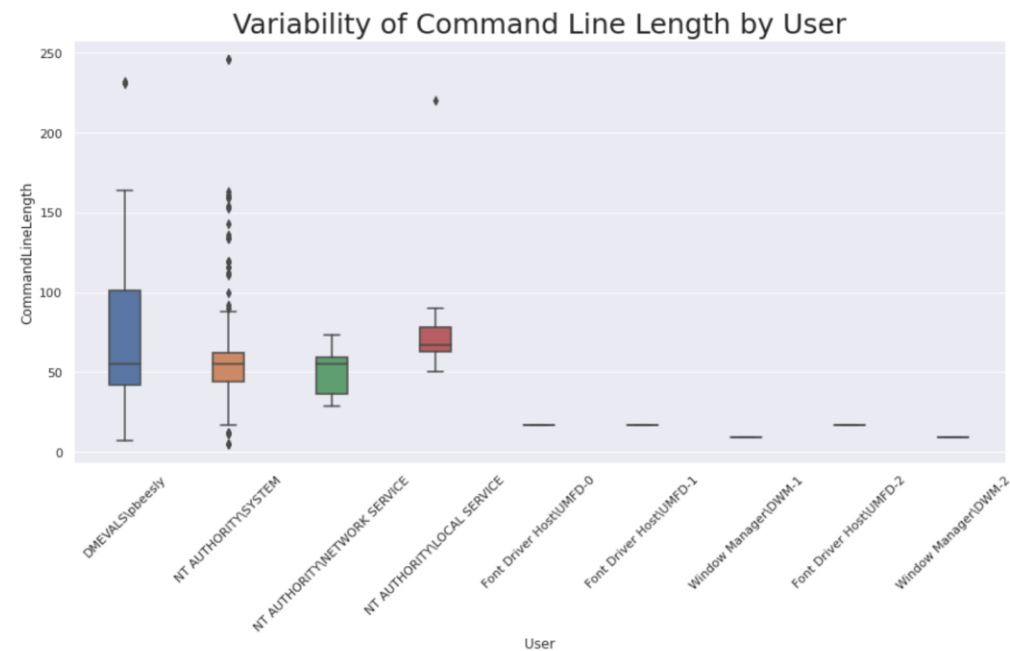
What Can I Do?: Visualize

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

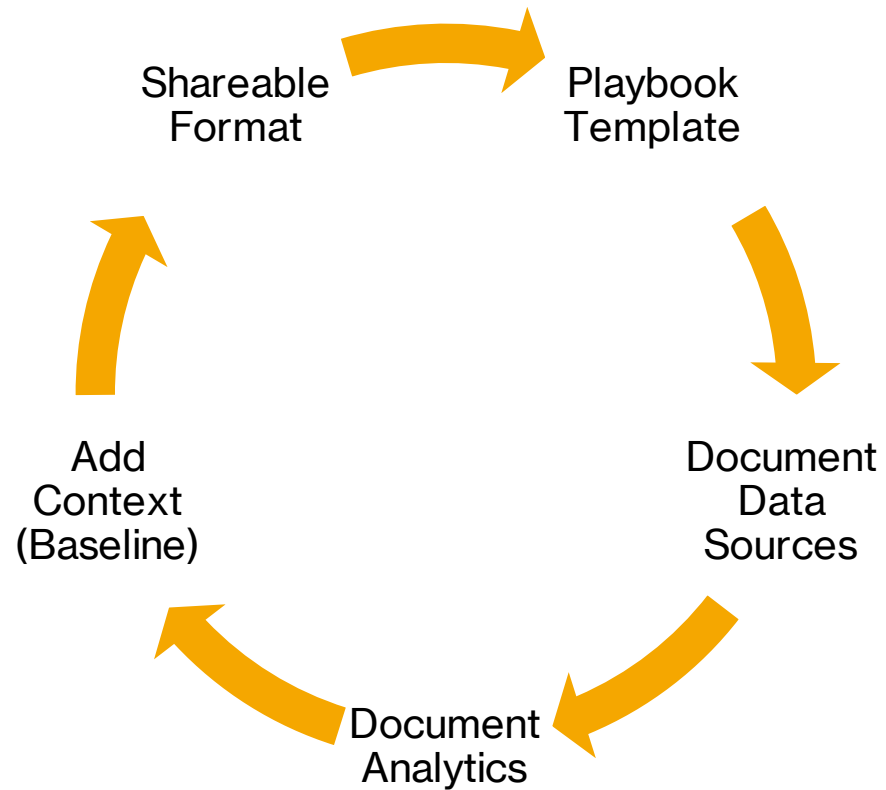
# seaborn object
boxPlotChart = sns.boxplot(x = 'User', y = 'CommandLineLength', data = source, orient = 'v', width=0.8)

# 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

Windows

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 Conections
Registry
WDigest Downgrade



Windows

ATT&CK Navigator View

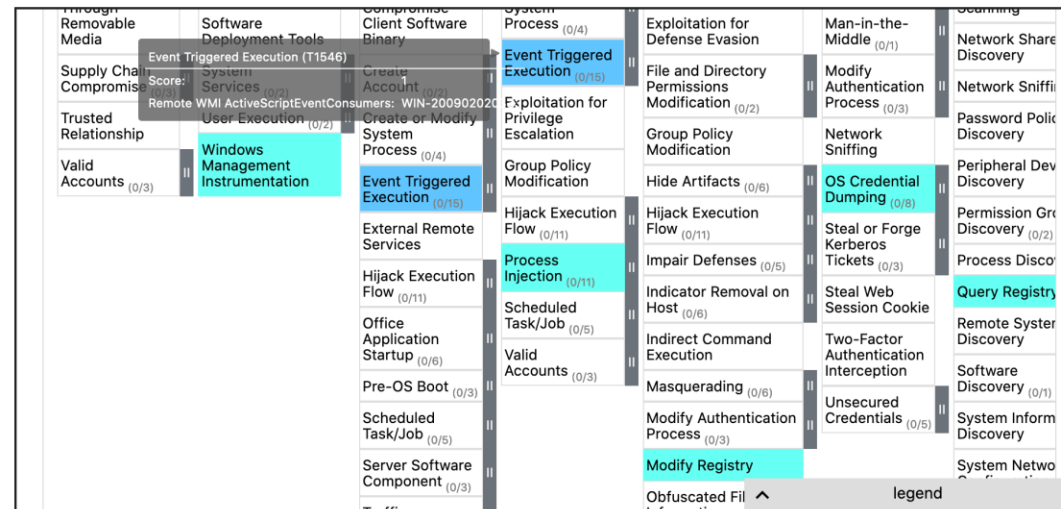


Table View

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

<https://github.com/OTRF/ThreatHunter-Playbook>

Document & Validate Detection

CreateRemoteThread and LoadLibrary
Enable Remote Desktop Conections
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\\\\scrrun.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

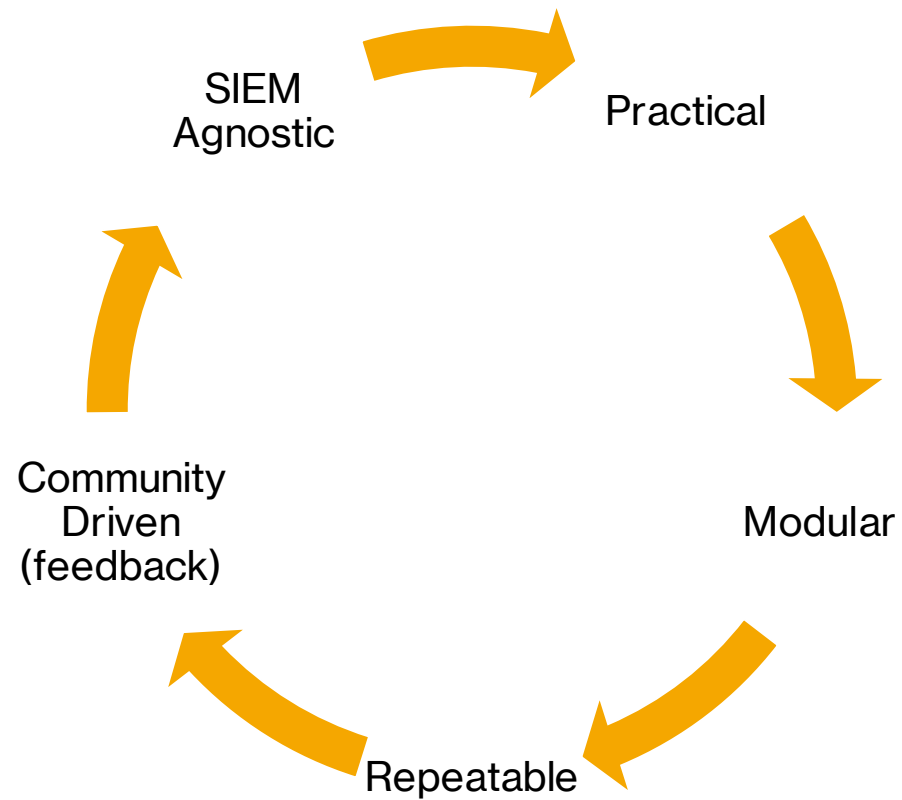
Hunter Notes

Hunt Output

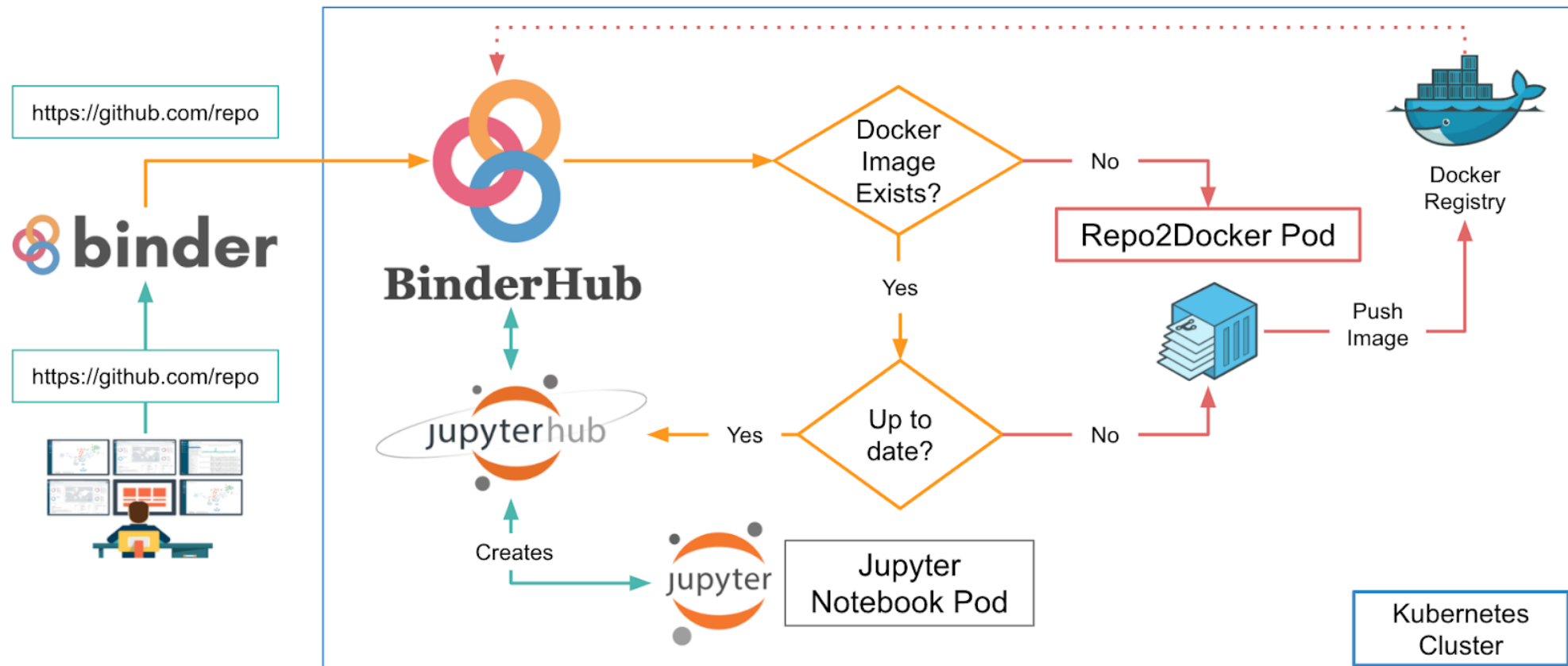
References

https://threathunterplaybook.com/notebooks/windows/08_lateral_movement/WIN-200902020333.html

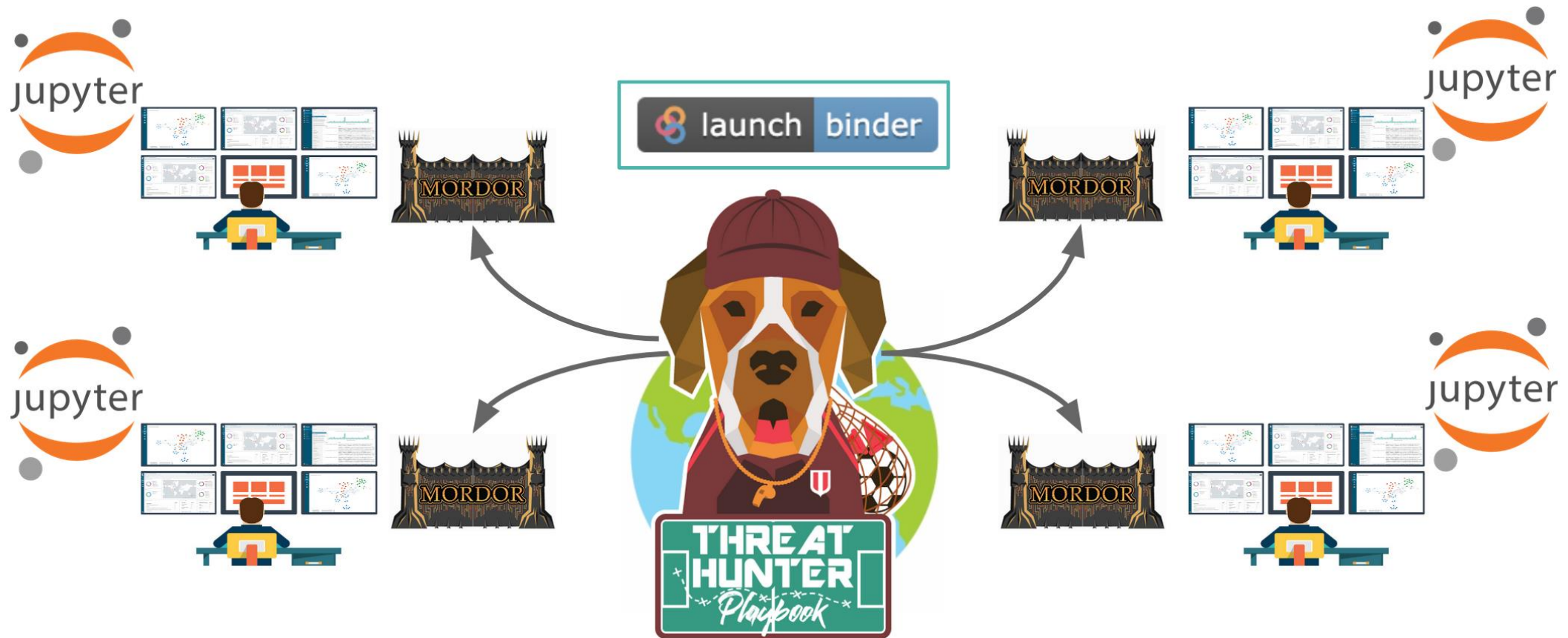
Share Your Research!



Repeatable? Practical? SIEM Agnostic?








Repeatable? Practical? SIEM Agnostic?



Repeatable? Practical? SIEM Agnostic?



Repeatable? Practical? SIEM Agnostic?



Remote WMI ActiveScriptEventConsumer

Launch Binder

Binder

Colab

Live Code

Metadata

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

Contents

Metadata

Technical Description

Hypothesis

Analytics

Detection Blindspots

Hunter Notes

Hunt Output

References

Repeatable? Practical? SIEM Agnostic?



Starting repository: OTRF/ThreatHunter-Playbook/master

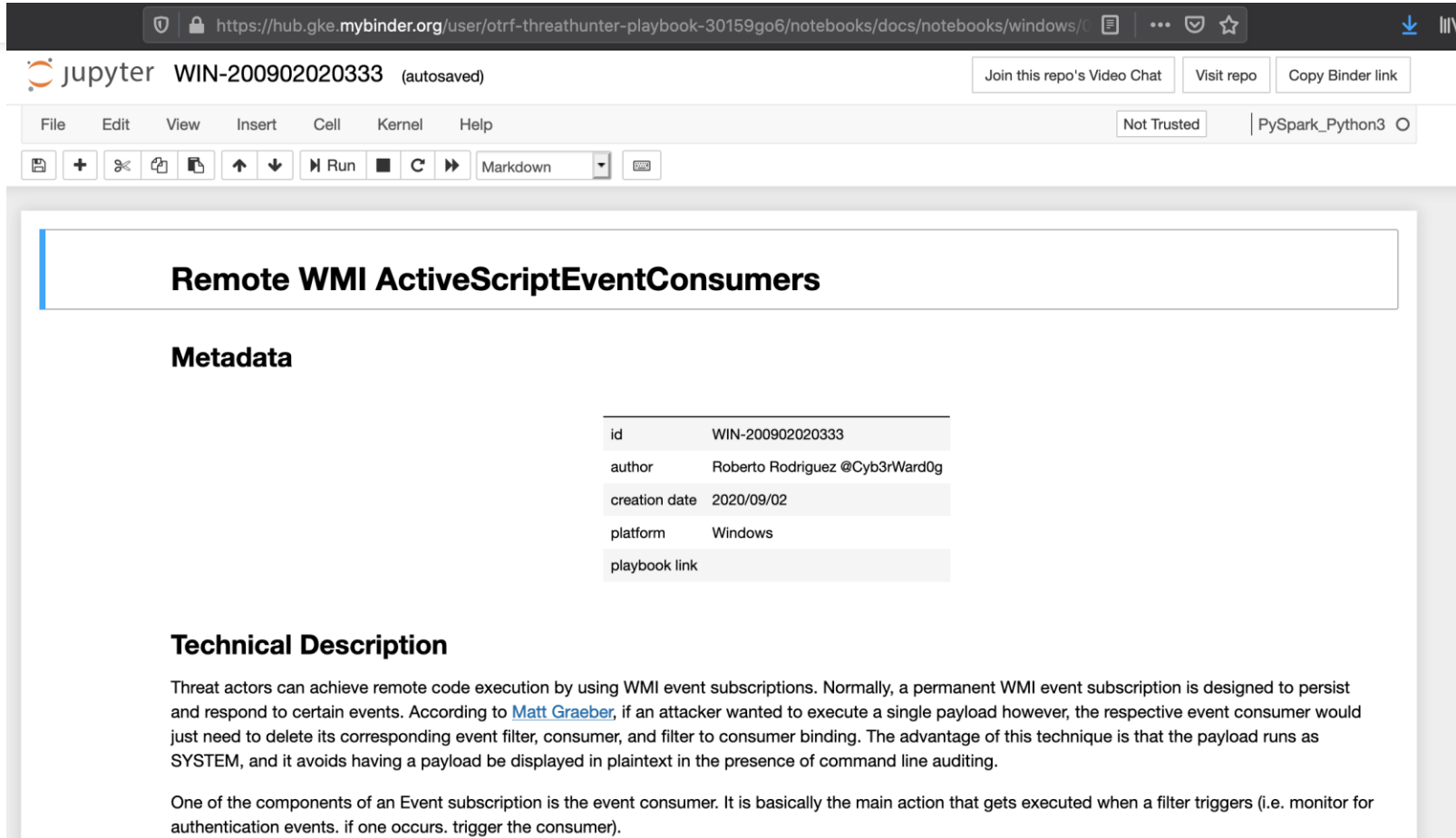
If a repository takes a long time to launch, it is usually because Binder needs to create the environment for the first time.

Build logs

[hide](#)

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


Repeatable? Practical? SIEM Agnostic?



The screenshot shows a Jupyter Notebook interface in a web browser. The address bar displays the URL: <https://hub.gke.mybinder.org/user/otrf-threathunter-playbook-30159go6/notebooks/docs/notebooks/windows/>. The notebook title is "WIN-200902020333 (autosaved)". The interface includes a menu bar (File, Edit, View, Insert, Cell, Kernel, Help) and a toolbar with icons for saving, adding cells, undo, redo, and running code. The notebook content is displayed in a markdown format.

Remote WMI ActiveScriptEventConsumers

Metadata

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

Technical Description

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?

jupyter WIN-200902020333 (autosaved) [Join this repo's Video Chat](#) [Visit repo](#) [Copy Binder link](#)

File Edit View Insert Cell Kernel Help Not Trusted | PySpark_Python3

Run

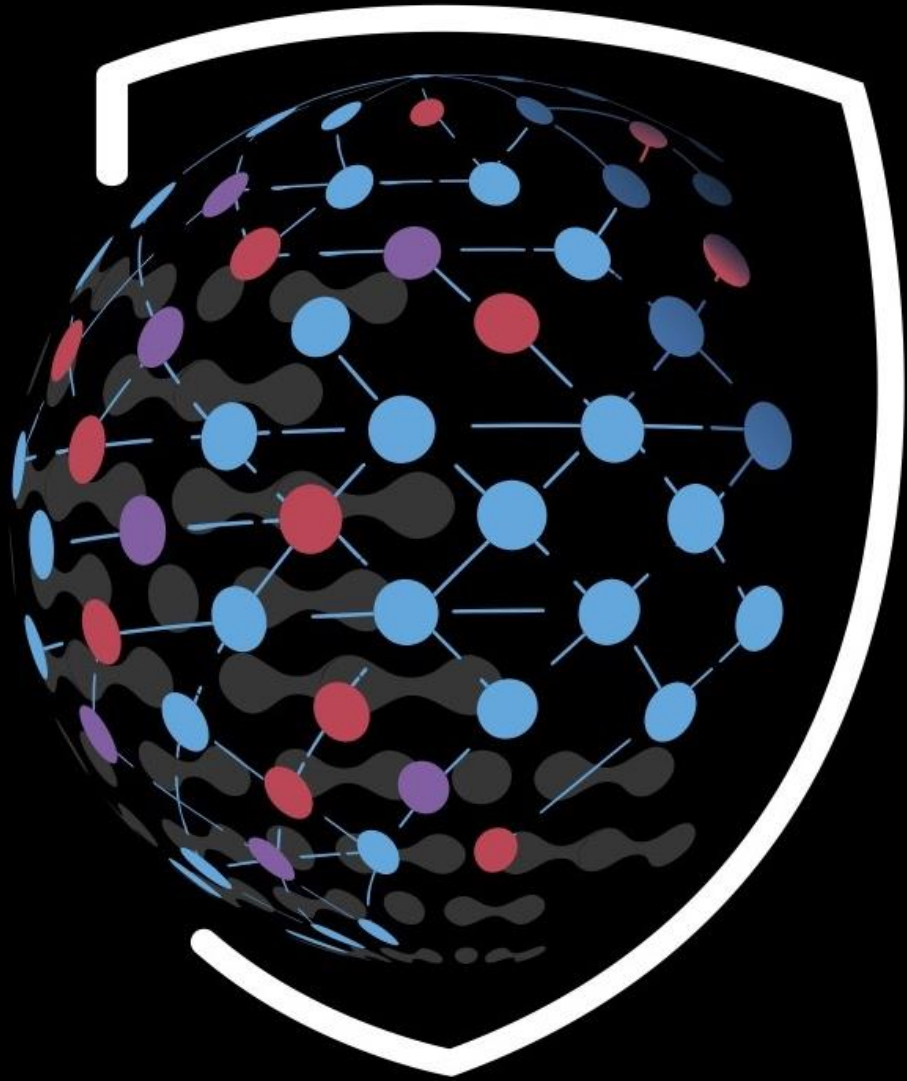
FP Rate	Log Channel	Description
Medium	['Microsoft-Windows-Sysmon/Operational']	Look for any indicators that the WMI script host process %SystemRoot%\system32\wbem\scrcons.exe is being used. You can do this by looking for a few modules being loaded by a process.

```
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)
```

Image	ImageLoaded	Description	ProcessGuid
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{c4e35f20-f8ea-5f4e-c504-000000000400}
C:\Windows\System32\wbem\scrcons.exe	C:\Windows\System32\wbem\scrcons.exe	WMI Standard Event Consumer - scriptin	{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 ??