

OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY



Bienvenidos a Mordor

Compartiendo data para Investigación y Detección de Amenazas con la Comunidad!

Quiénes Somos?



Fundadores de Open Threat Research!

Roberto Rodriguez 
@Cyb3rWard0g

- Microsoft Threat Intelligence Center (MSTIC)

Jose Rodriguez 
@Cyb3rPandaH

- MITRE - ATT&CK

- Colaboración y Código Abierto 
- [@OTR_Community](#)
- Threat Hunter Playbook
[@HunterPlaybook](#)
- Mordor [@Mordor_Project](#)
- OSSEM [@OSSEM_Project](#)
- Blacksmith & more..

Agenda

- 1) Que motiva R&D de una Detección?
- 2) Una Metodología Basica
- 3) Simulando al Adversario
 - Beneficios y Desafíos
- 4) Bienvenidos a Mordor!!
 - Como se origino?
 - Set de datos para todo el mundo
 - Diseño de ambiente de prueba
 - Qué podemos hacer con los datos?
- 5) Lo que se viene con Mordor



Qué Motiva R&D de una Detección?

Investigación y Desarrollo desde
Casa!



Hoy en día...

 **MDSec** @MDSecLabs

Part 1 in the "I Like to Mo @domchell is now live... [t](#)



9:26 AM · Sep 1, 2020 · Twitter

120 Retweets 4 Quote Tweets

6 1

Dwight Hohnstein @djhohnstein

My first blog on abusing the Service Control Manager and DLL hijacks for lateral movement. I cover methodology, detections and proof of concept code. Thanks to @mattifestation/@Cyb3rWard0g for all their detection contributions!

Process Monitor Filter

Filters were in effect the last time you exited Process Monitor:

Display entries matching these conditions:

Architecture	is	
Reset		

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Result	is	NAME NOT FOUND	Include
<input checked="" type="checkbox"/> User	is	NT AUTHORITY\SYSTEM	Include
<input checked="" type="checkbox"/> Path	ends with	sys	Include
<input checked="" type="checkbox"/> Path	ends with	dll	Include

Lateral Movement—SCM and Dll Hijacking Primer

Using the Service Control Manager and built-in services for lateral movement.



Benjamin Delpy  @gentilkiwi

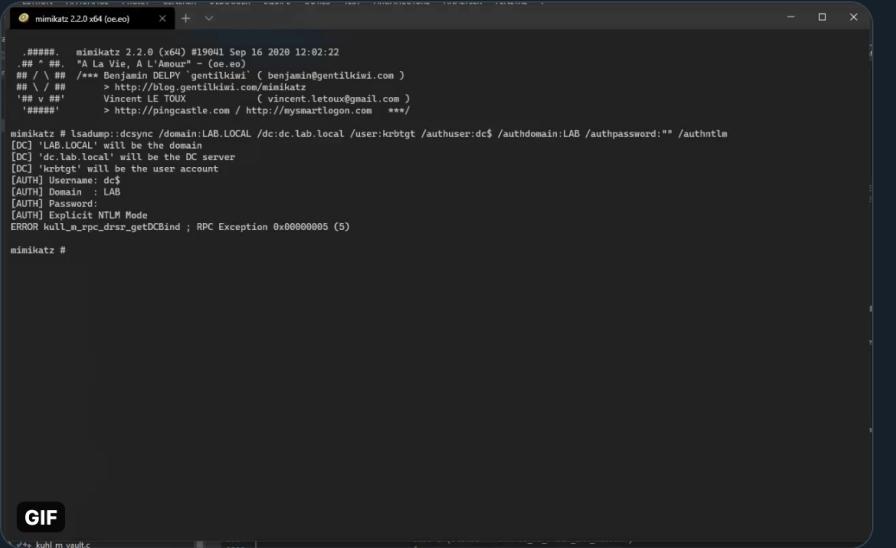
A new **#mimikatz**  release with **#zerologon** / CVE-2020-1472 detection, exploit, DCSync support and a lots of love inside 

It now uses direct RPC call (fast and supports unauthenticated on Windows)

> github.com/gentilkiwi/mim...

nt i art

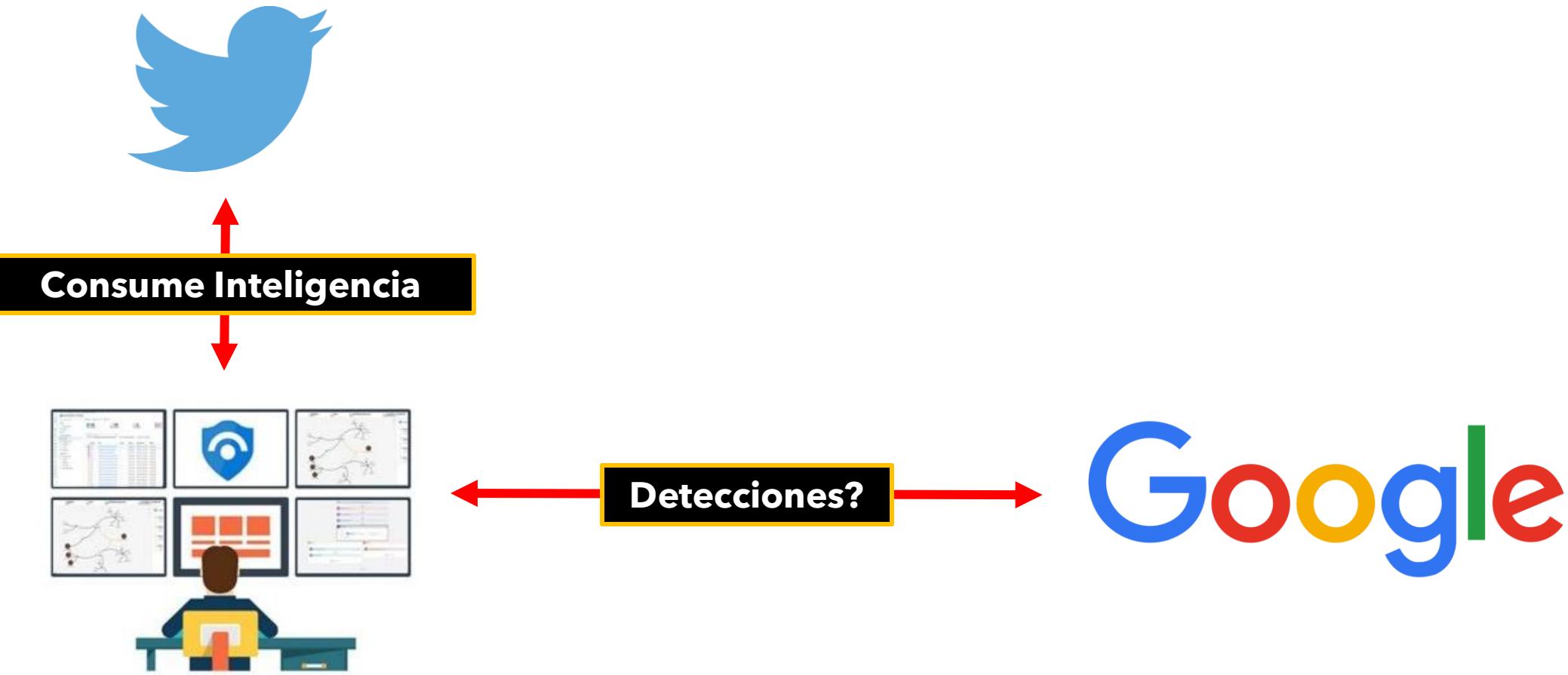
Thank you: @SecuraBV



6:30 AM · Sep 16, 2020 · Twitter Web App

643 Retweets 34 Quote Tweets 1K Likes

Qué hago? Alguien en la comunidad?



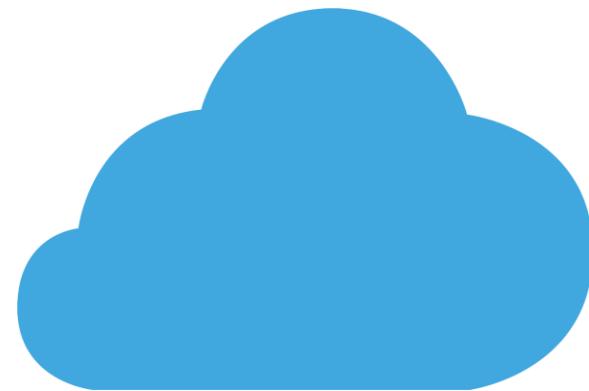
Lo Simulas de Una? Qué Necesitas?

Google

Cómo lo ejecuto?



Donde?



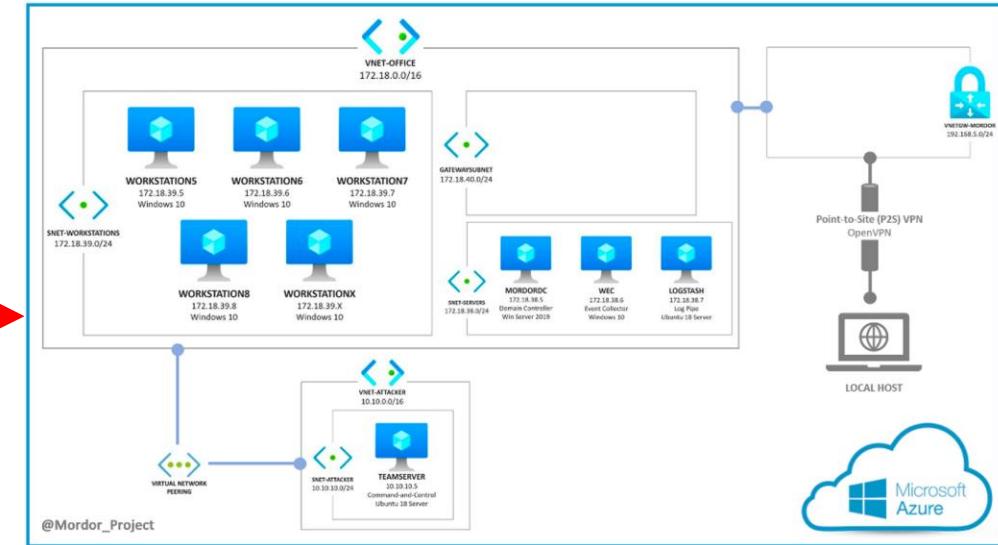
Requiero de una o más computadoras?

Google

Como lo ejecuto?



Dónde?

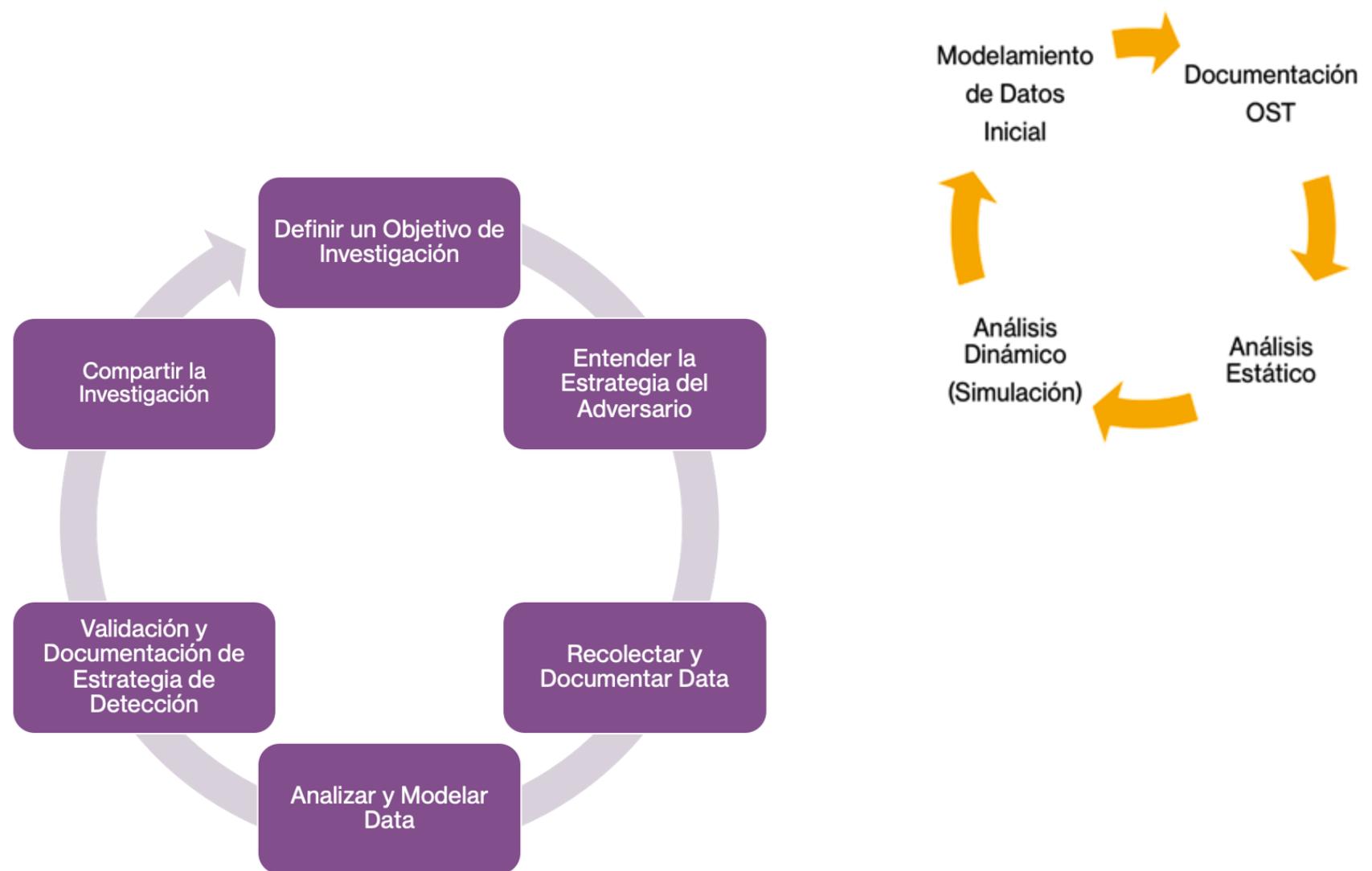


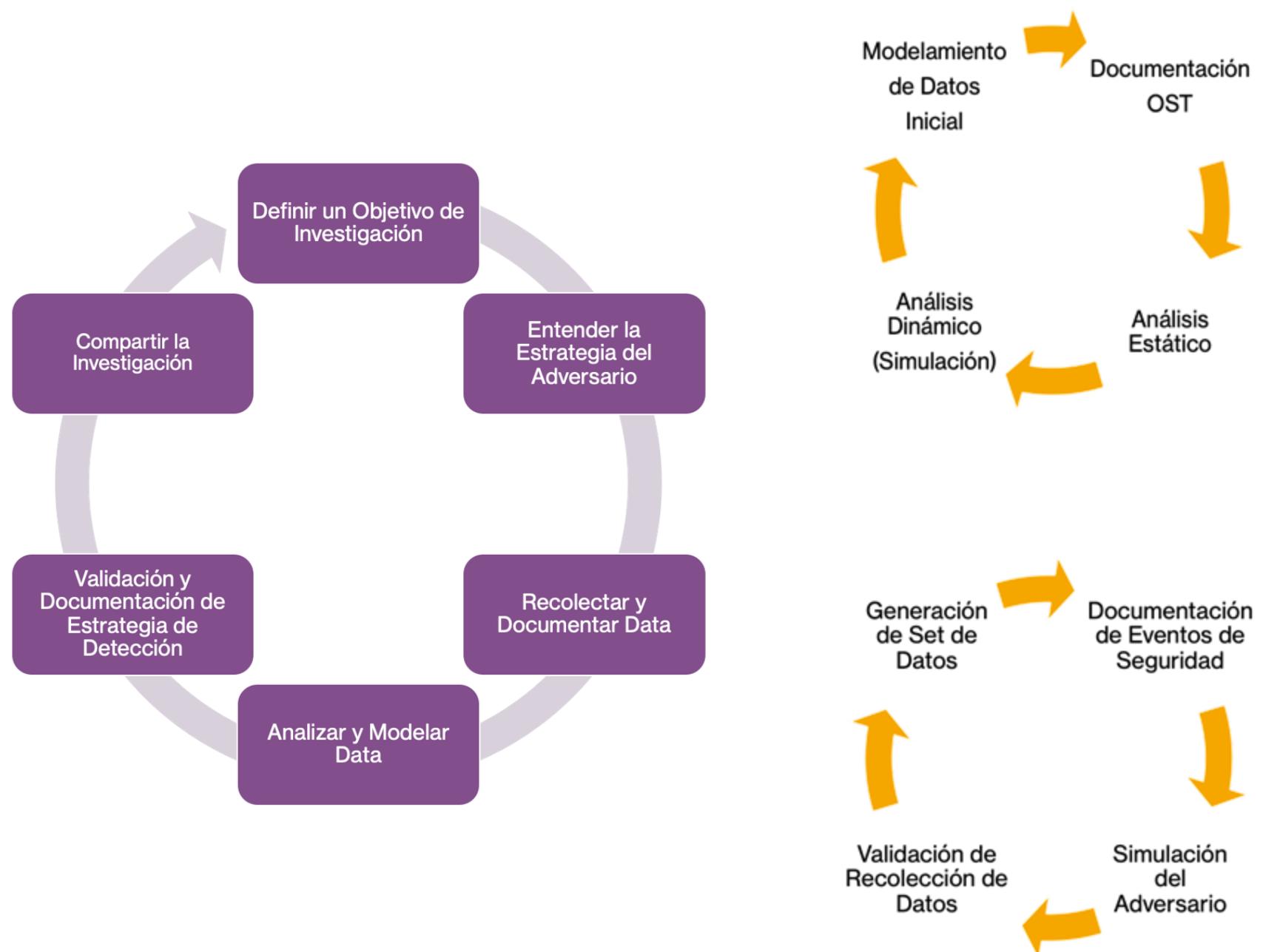
Una Metodología Básica!

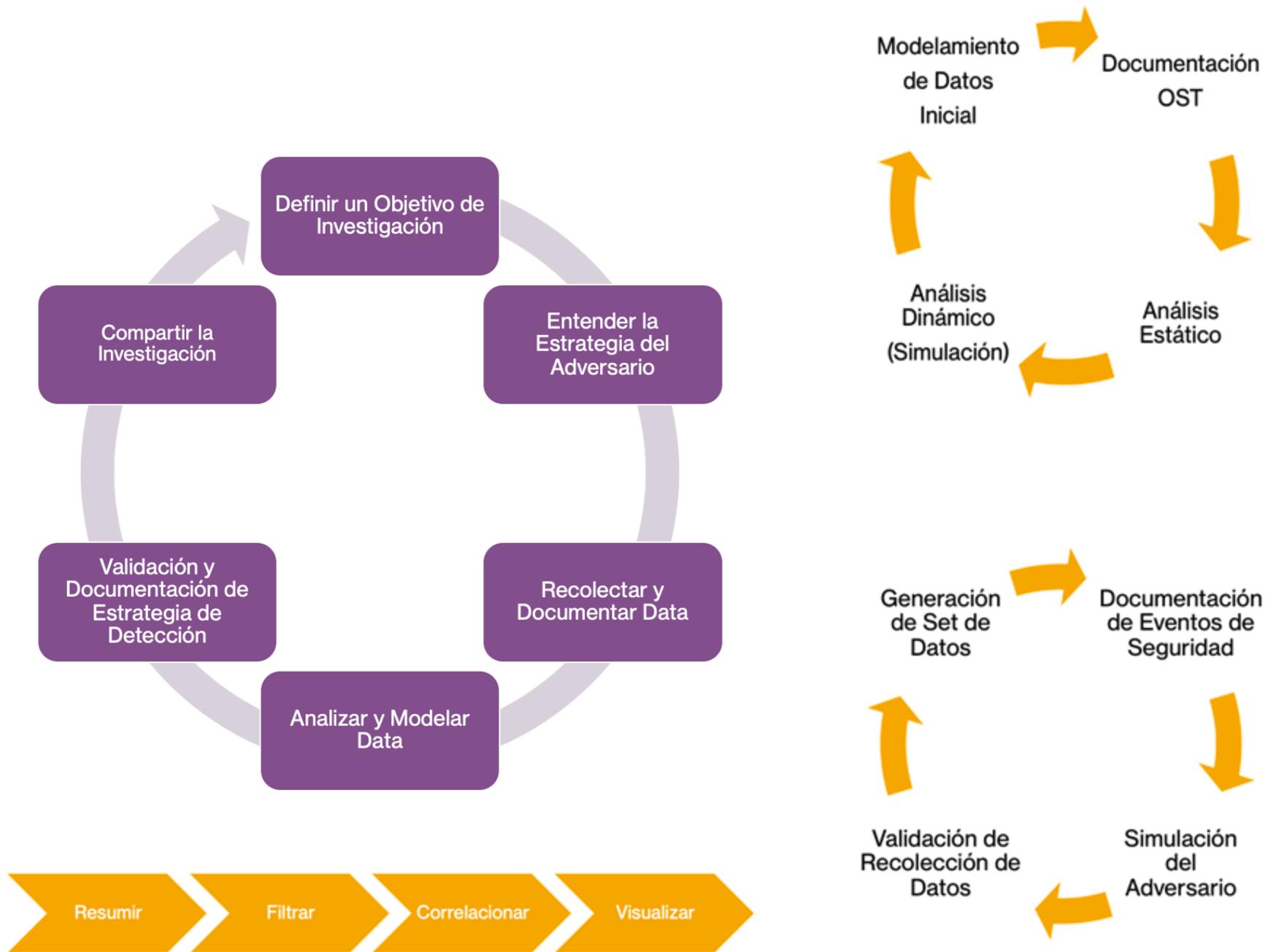
La que usamos! 😊

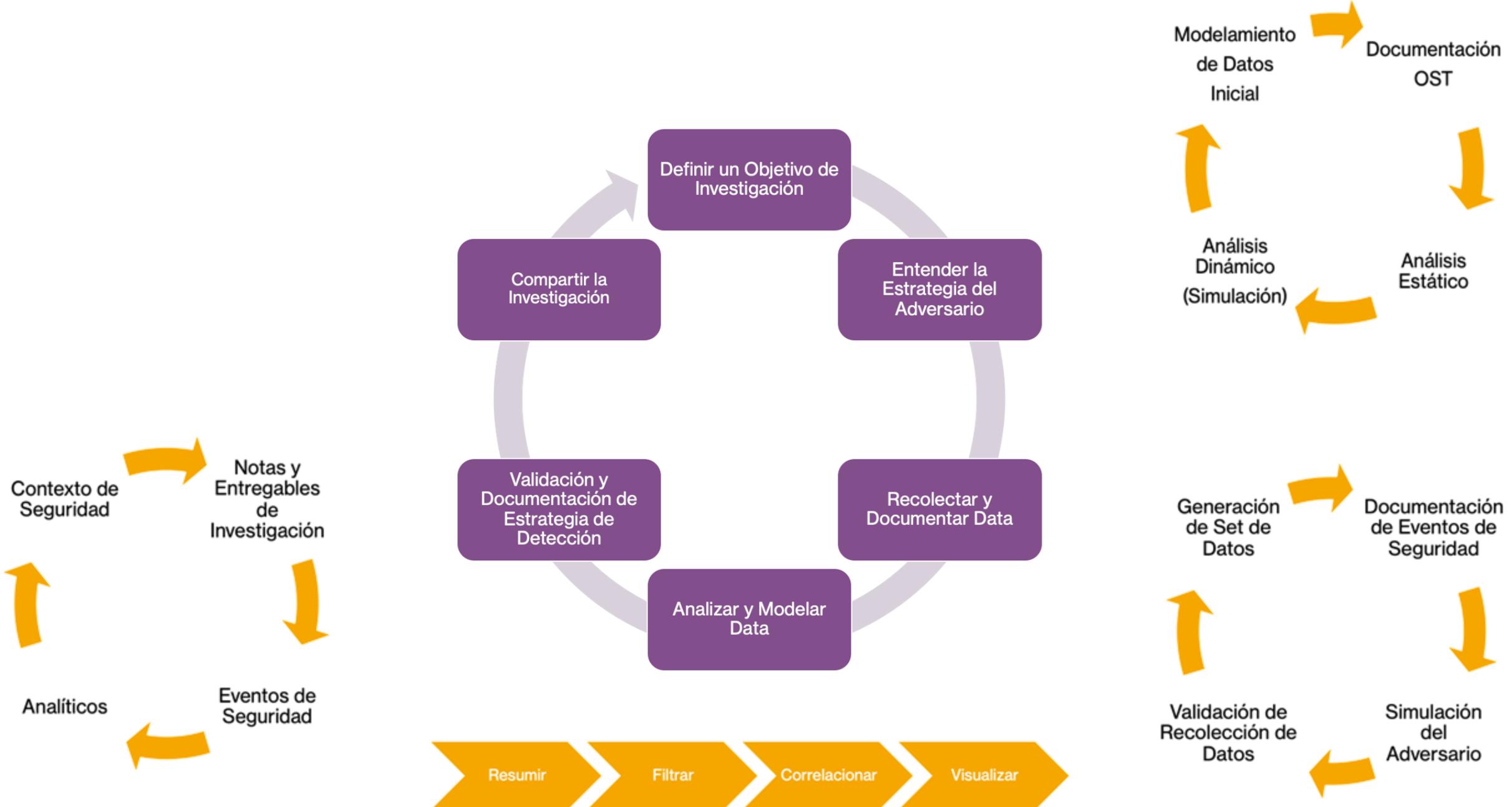


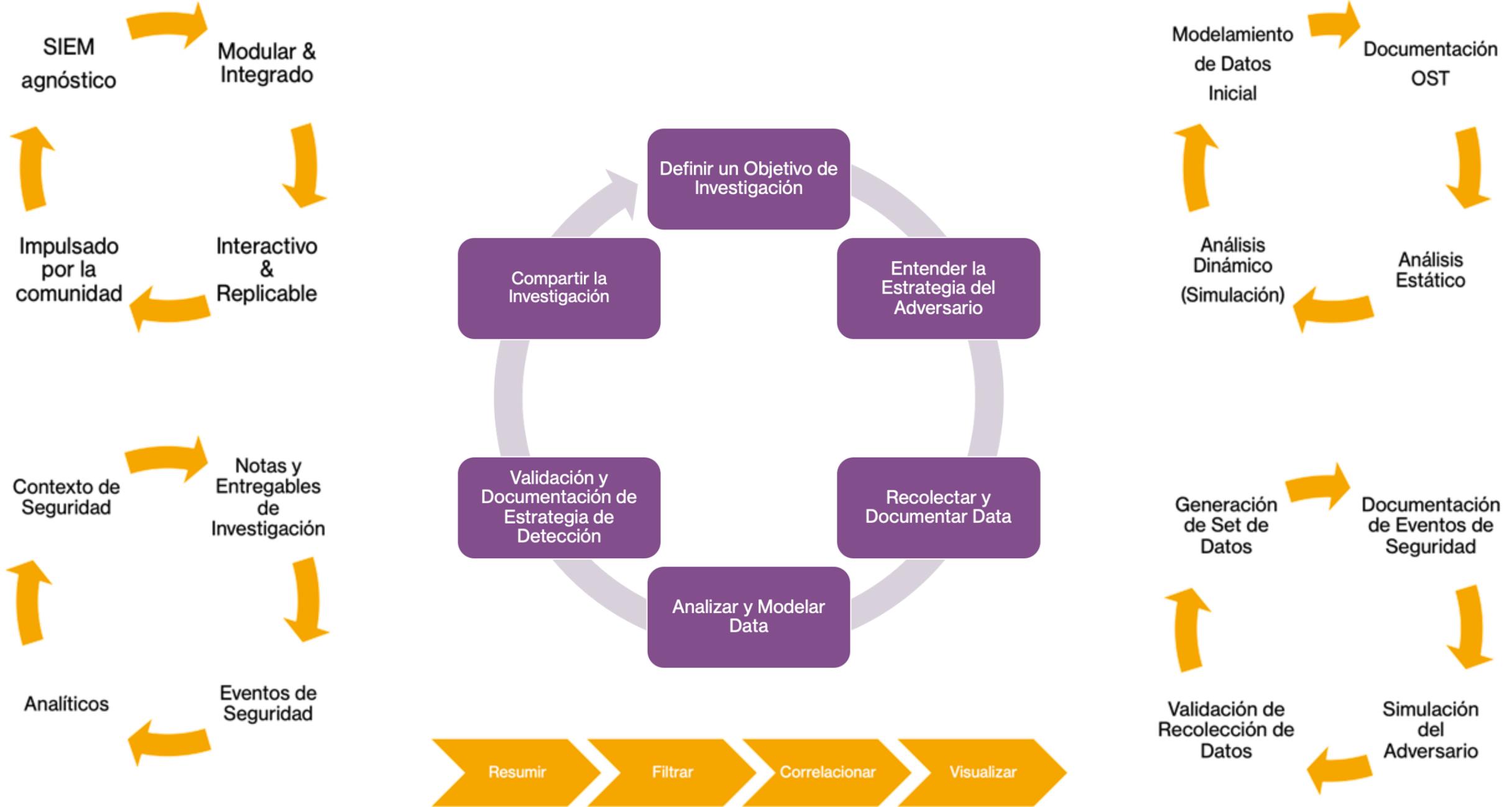














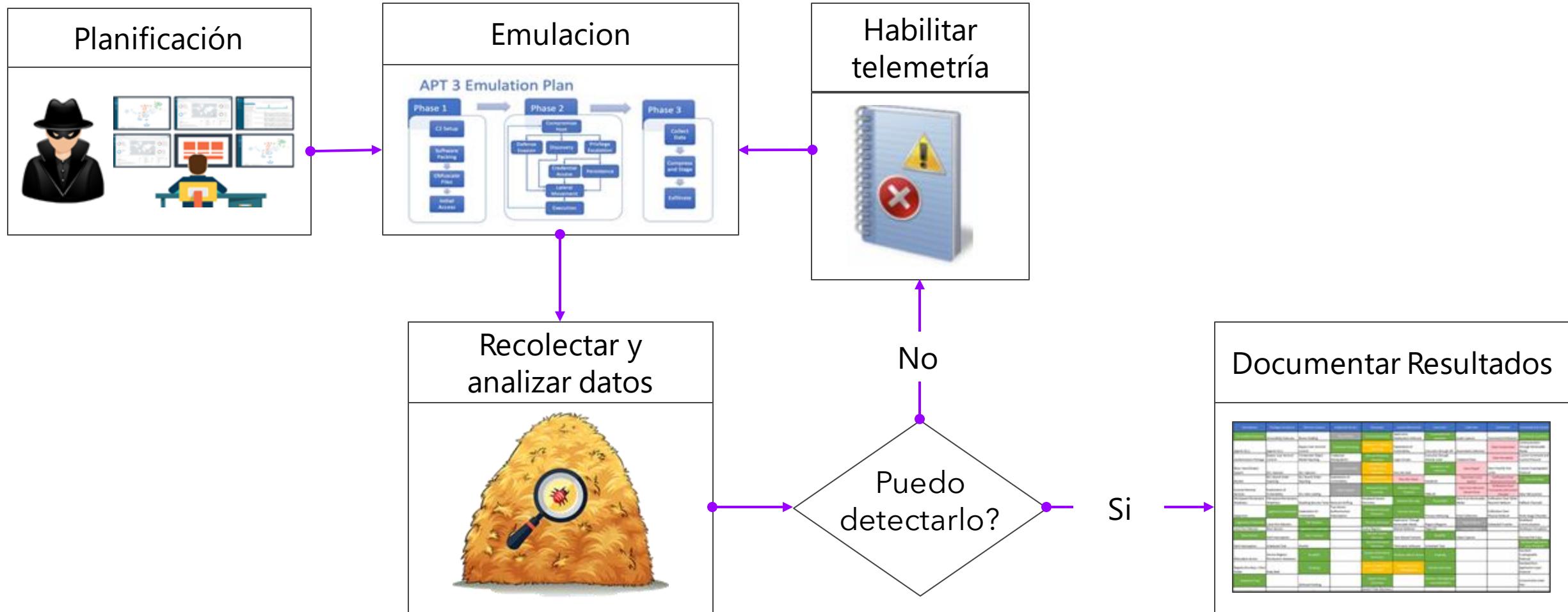


Simulando al Adversario!

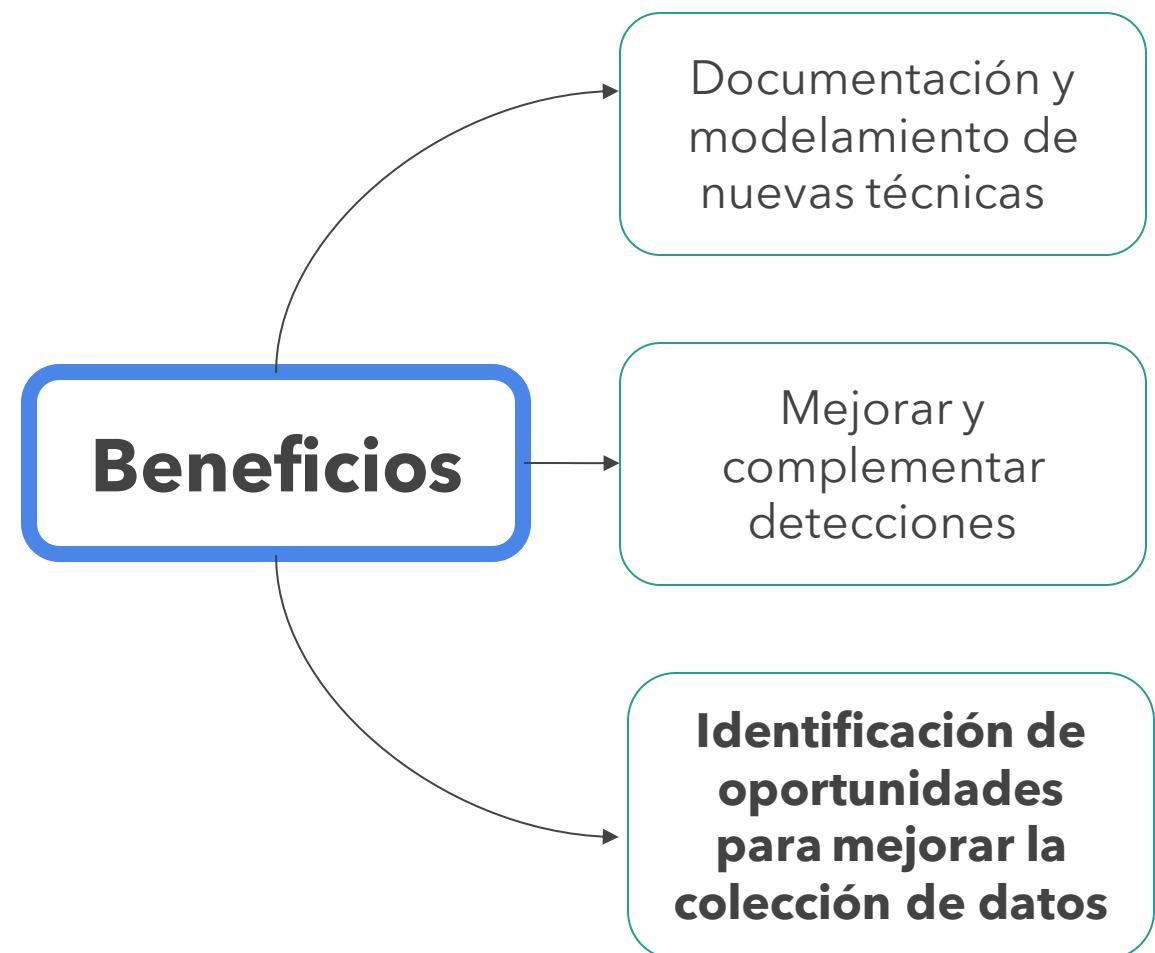
Desde casa!



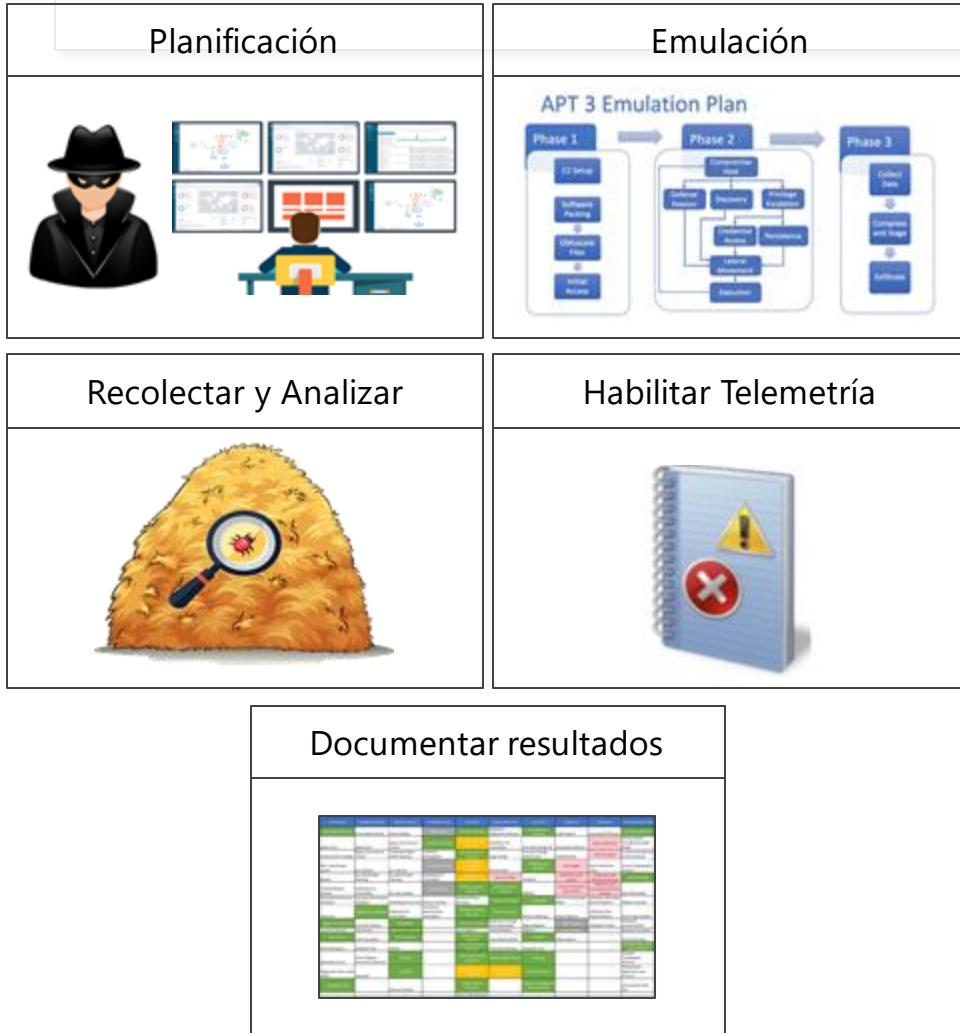
Actividades Básicas al simular al adversario



Más que validar controles de seguridad!!



Cómo? Dónde? Cuándo? Whát 🎉? (Spanglish)



Desafíos

Puede requerir alta inversión de **tiempo** y **tecnología**

Pueda que tengas que escribir tus propias herramientas

Configurar la colección de datos es más que un solo comando o switch

No nos crees 😈? Un ejemplo básico..

Dwight Hohnstein
@djhohnstein

My first blog on abusing the Service Control Manager and DLL hijacks for lateral movement. I cover methodology, detections and proof of concept code. Thanks to [@mattifestation](#)/[@Cyb3rWard0g](#) for all their detection contributions!

Process Monitor Filter

Filters were in effect the last time you exited Process Monitor:

Display entries matching these conditions:

Architecture	is	
--------------	----	--

Reset

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Result	is	NAME NOT FOUND	Include
<input checked="" type="checkbox"/> User	is	NT AUTHORITY\SYSTEM	Include
<input checked="" type="checkbox"/> Path	ends with	sys	Include
<input checked="" type="checkbox"/> Path	ends with	dll	Include

Lateral Movement—SCM and Dll Hijacking Primer
Using the Service Control Manager and built-in services for lateral movement.

Abusando de el SCM y DLL Hijacks!

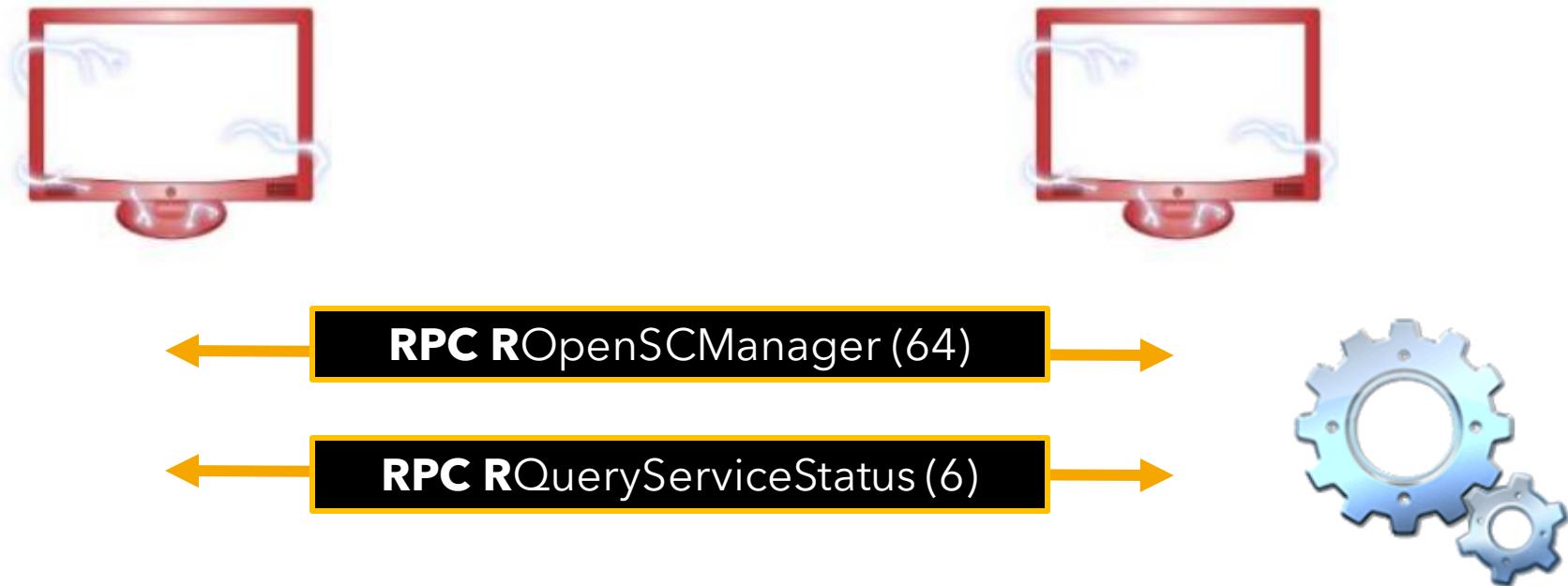


Abusando de el SCM y DLL Hijacks!

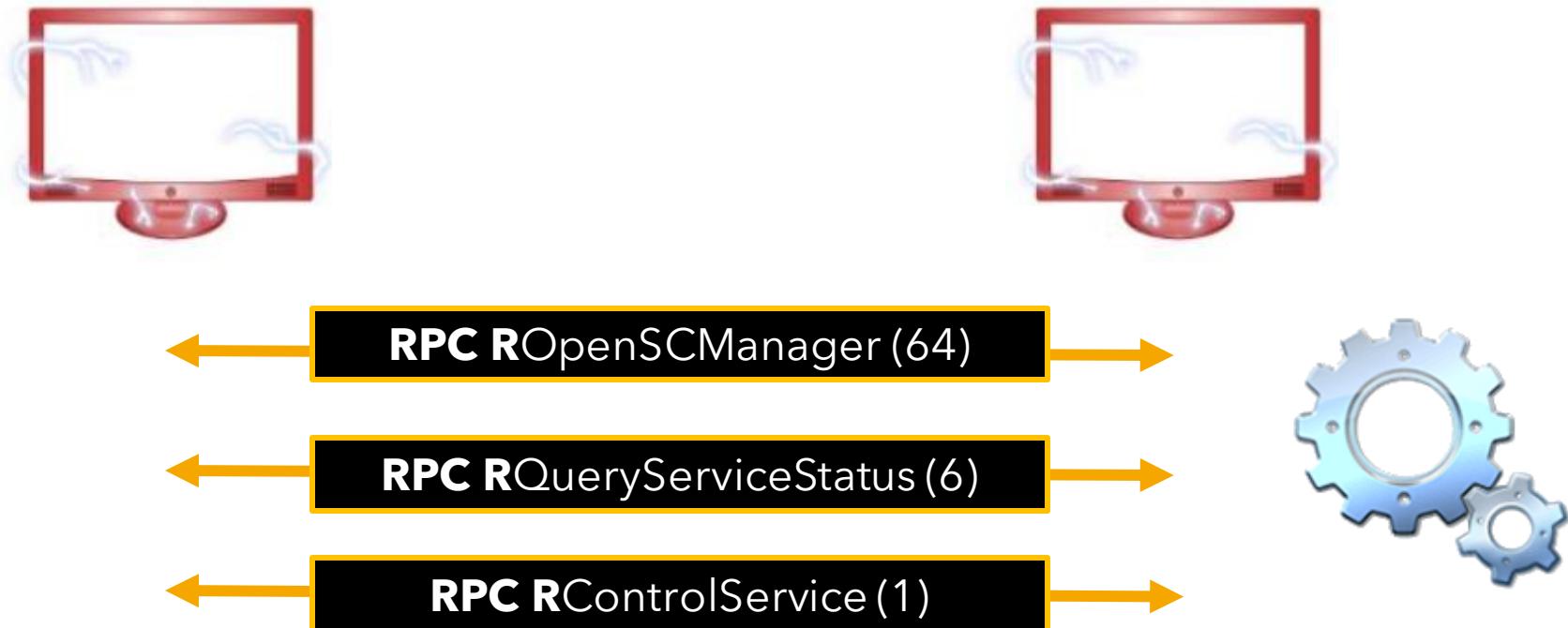


**Servicio Vulnerable
Identificado**

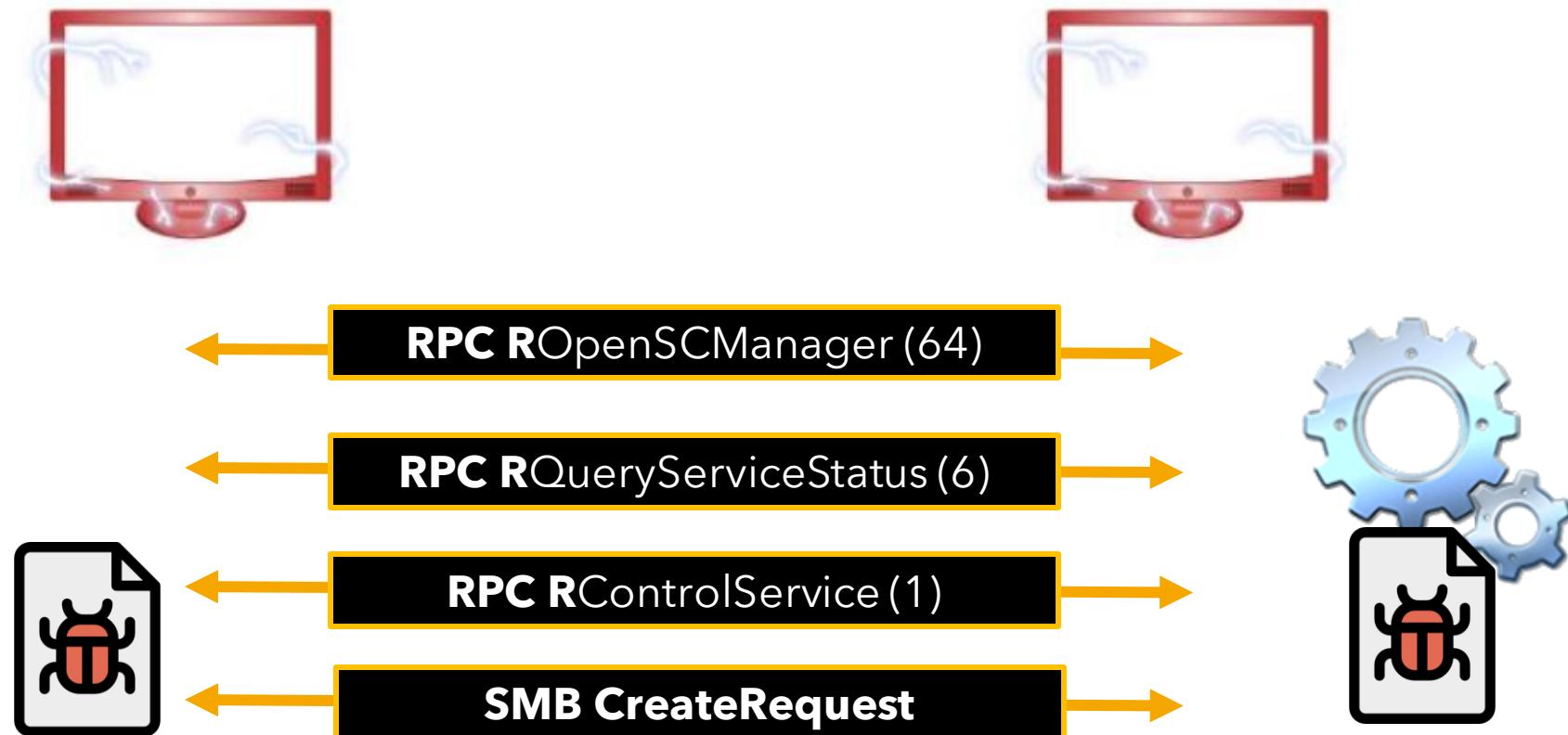
Abusando de el SCM y DLL Hijacks!



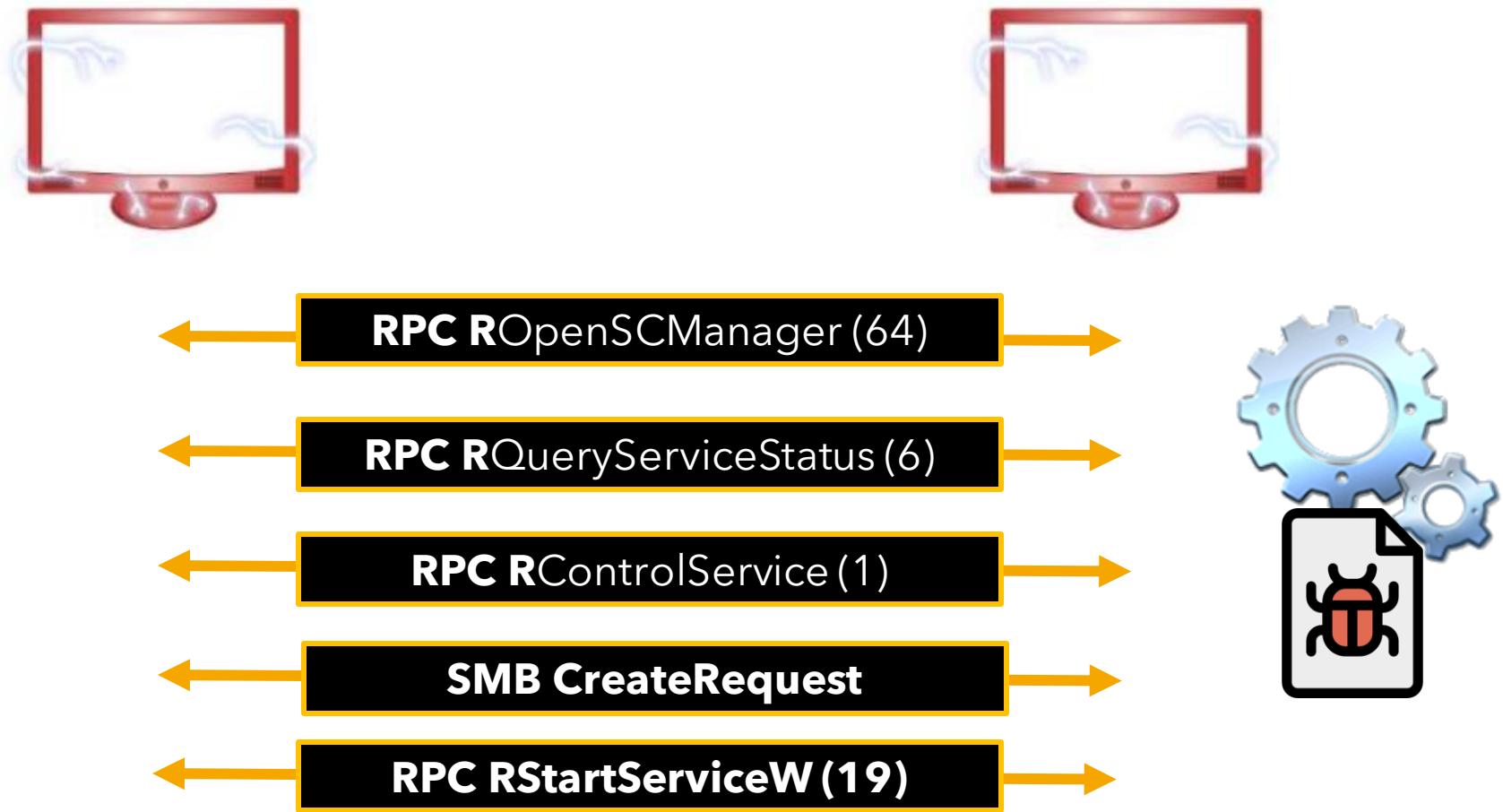
Abusando de el SCM y DLL Hijacks!



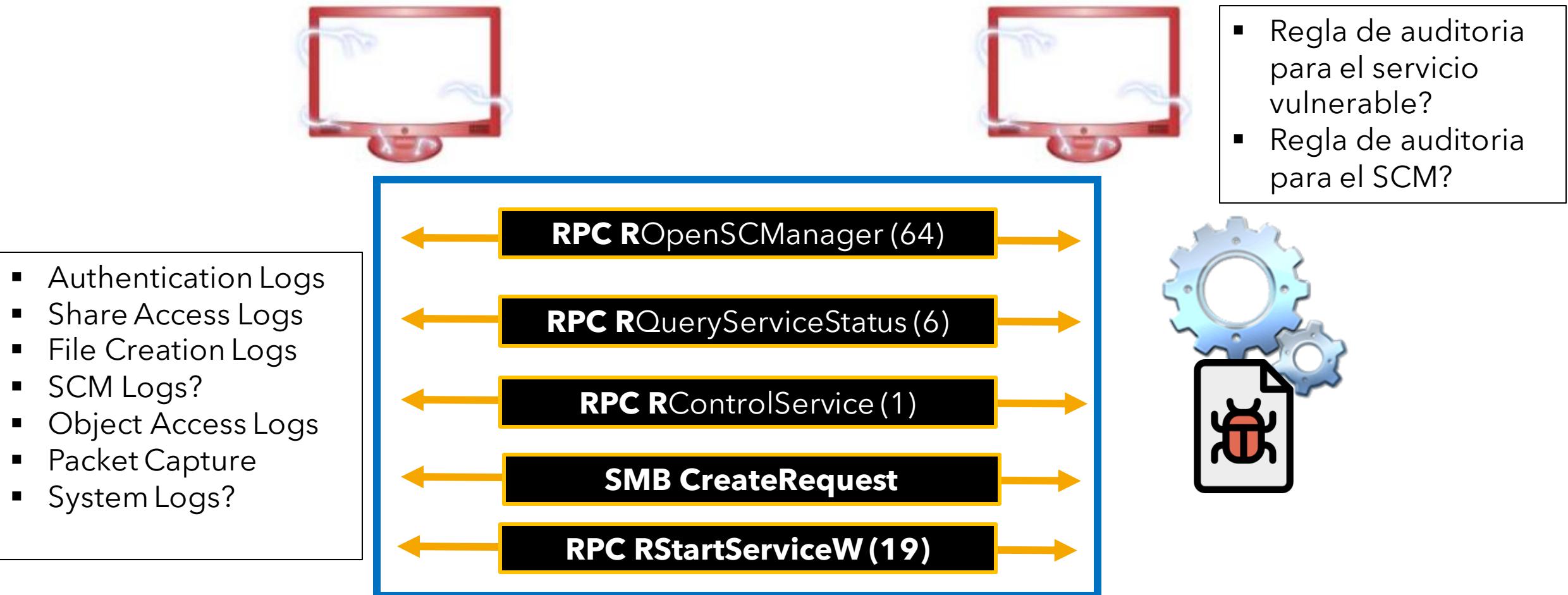
Abusando de el SCM y DLL Hijacks!



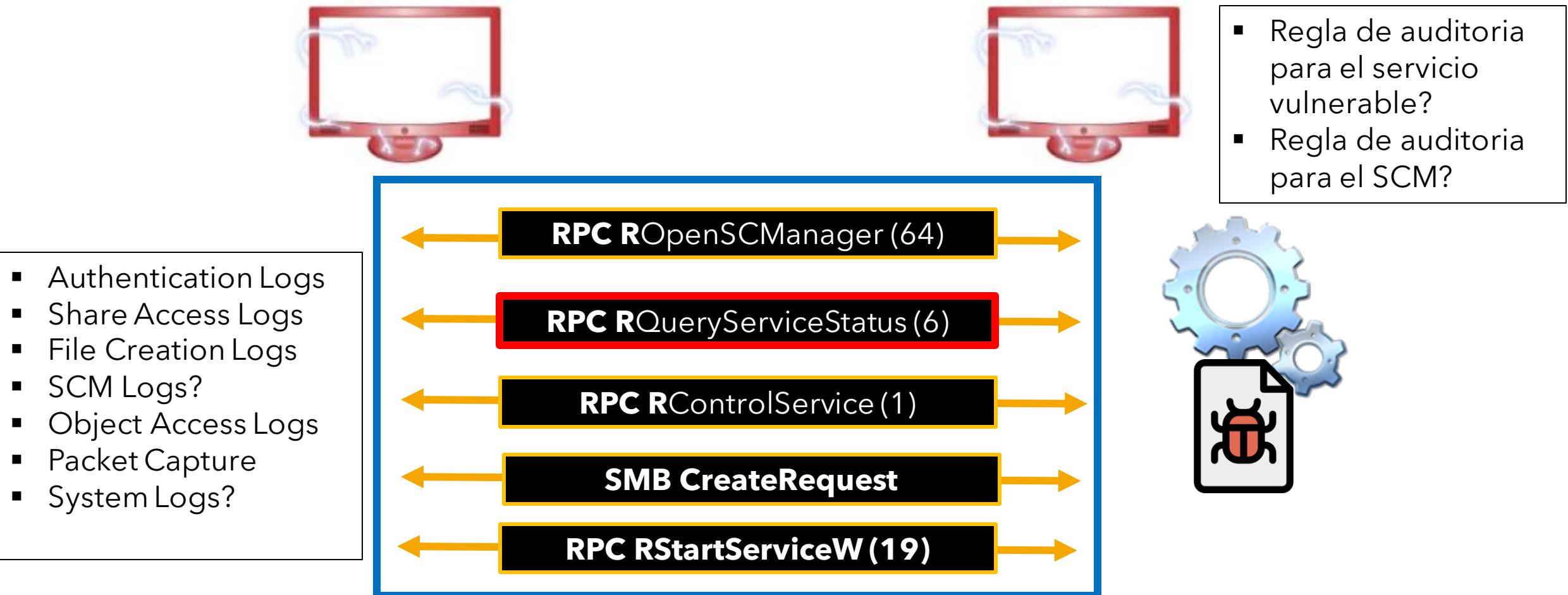
Abusando de el SCM y DLL Hijacks!



Qué necesito?: Pólizas de Auditoria



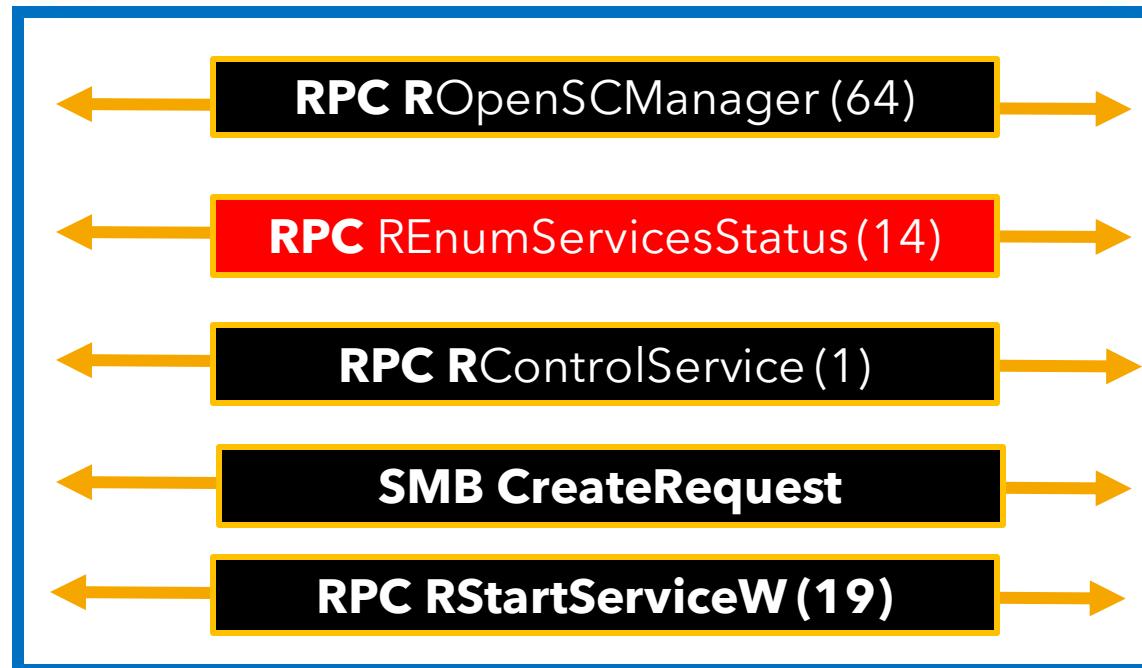
Cómo respondo a las variaciones?



Qué pasa si el servicio no es tocado?

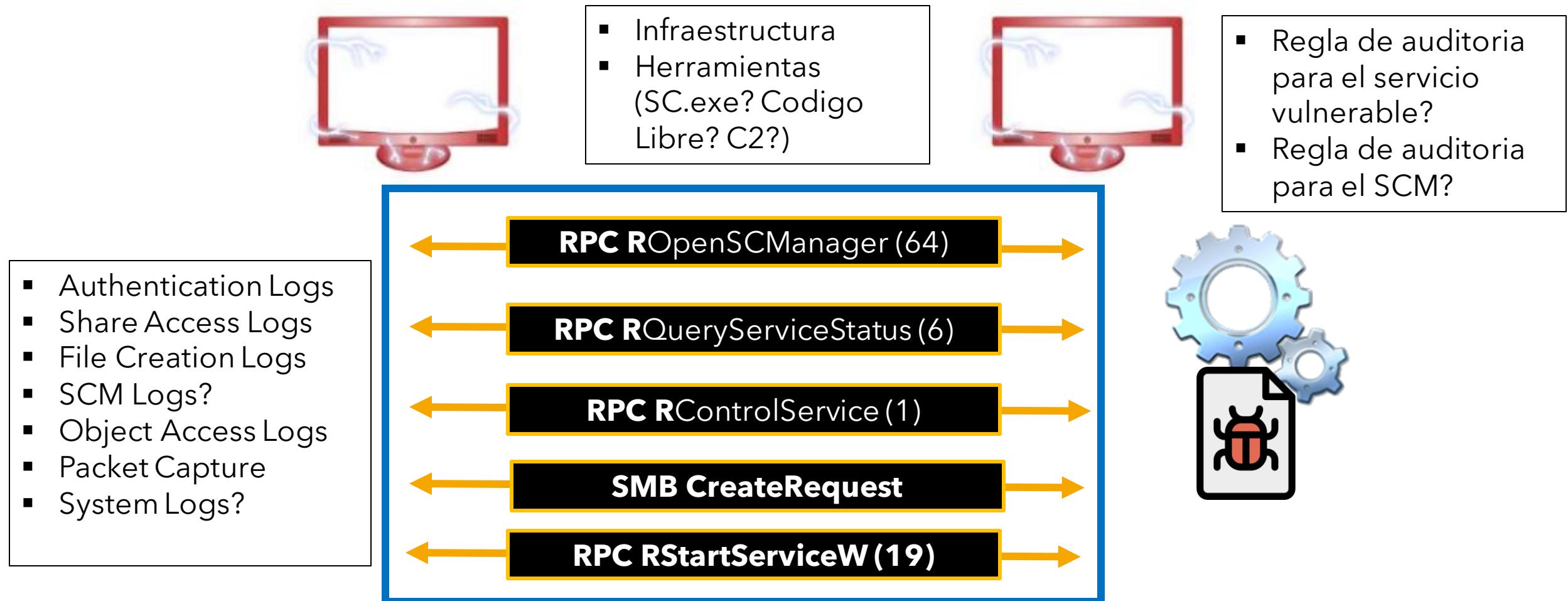


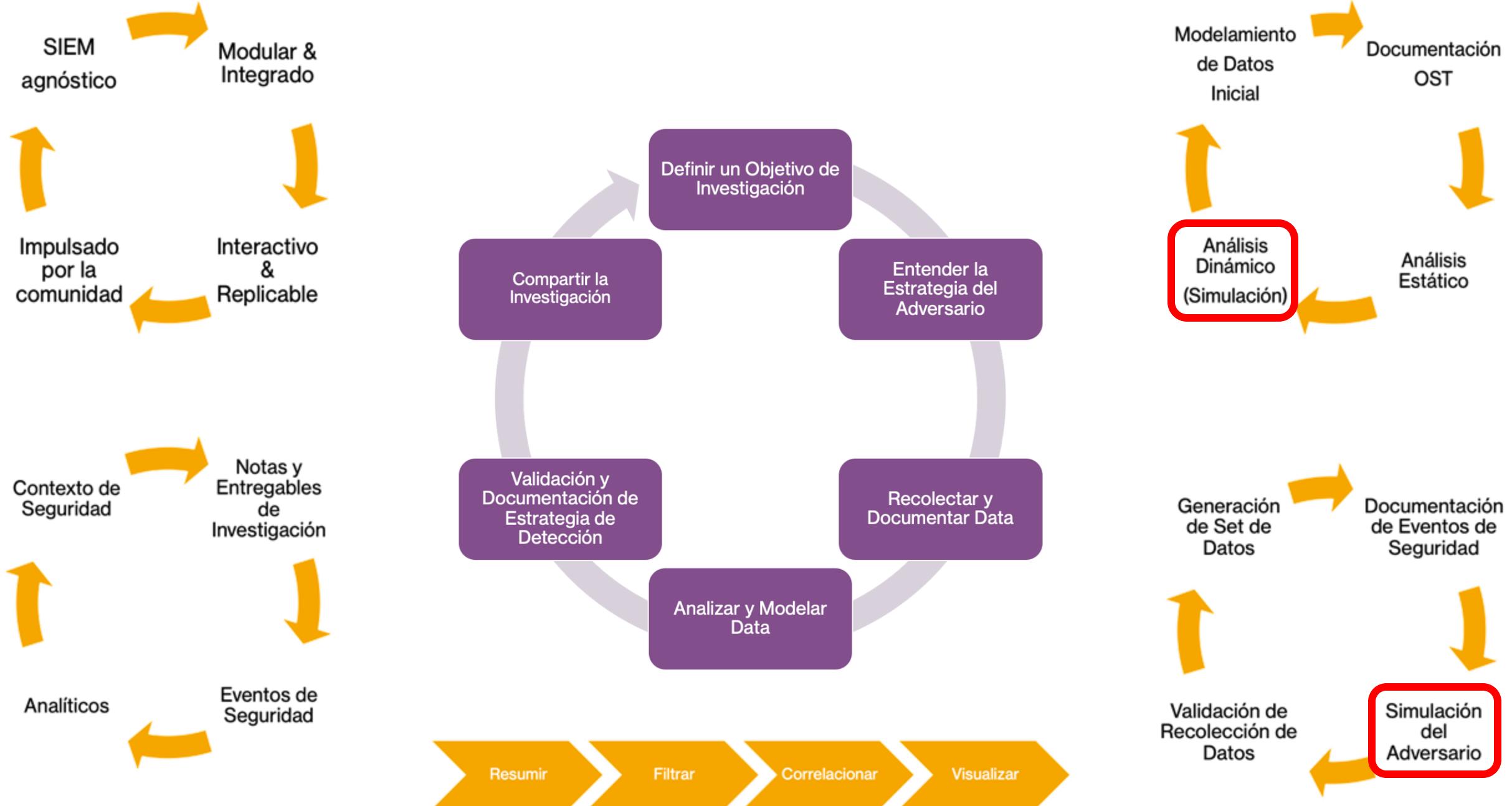
- Authentication Logs
- Share Access Logs
- File Creation Logs
- SCM Logs?
- Object Access Logs
- Packet Capture
- System Logs?



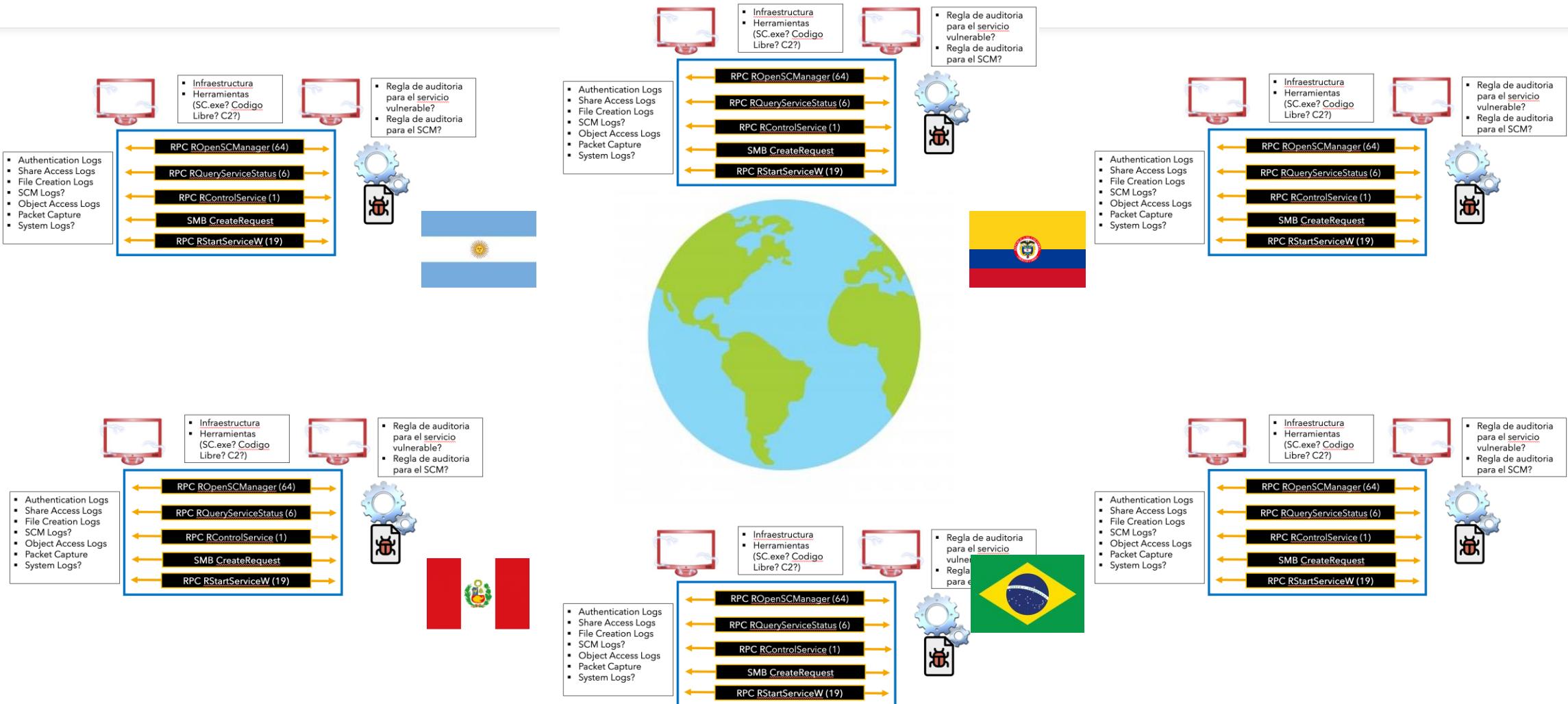
- Regla de auditoria para el servicio vulnerable?
- Regla de auditoria para el SCM?

Qué herramientas? Qué infraestructura?

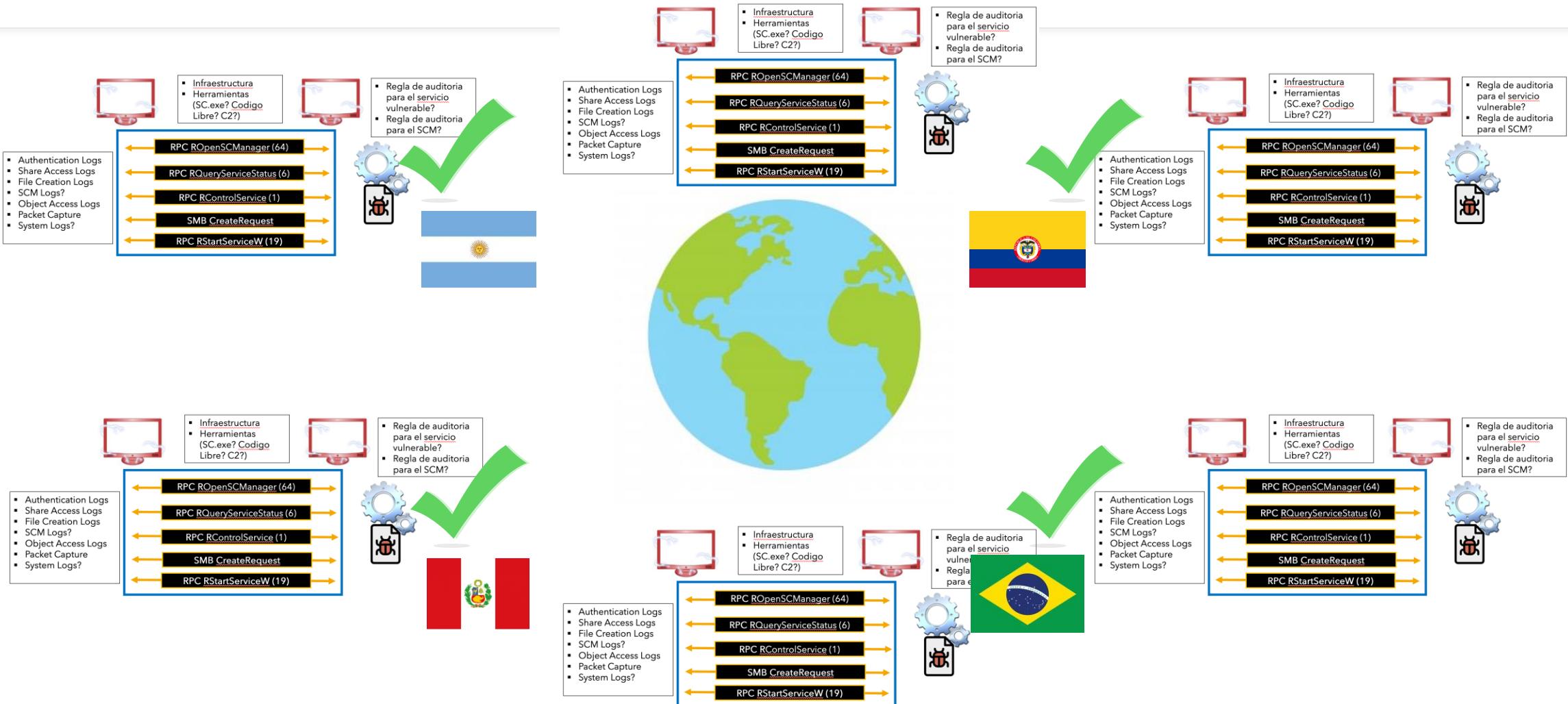




En todas partes de el mundo...

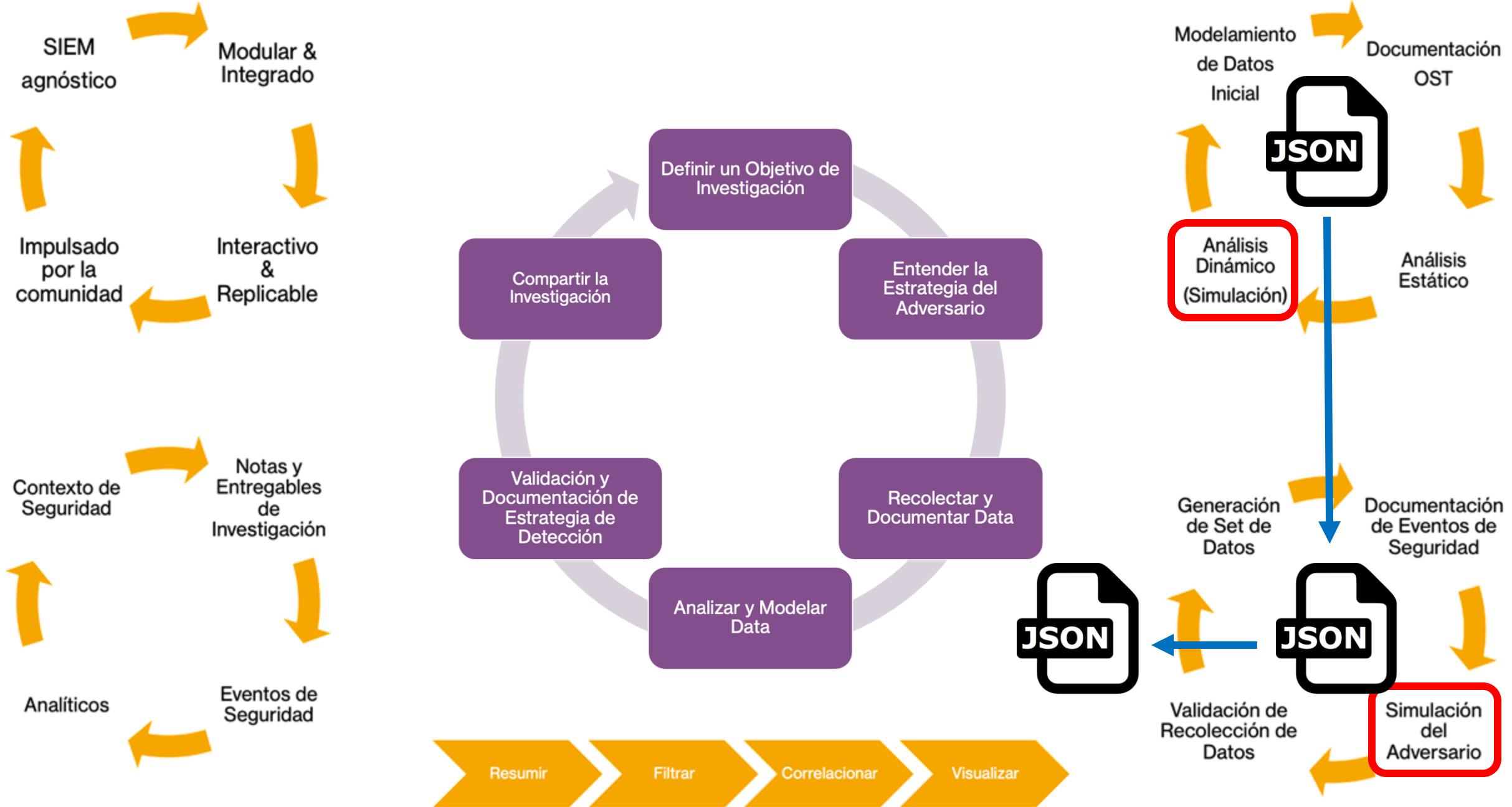


En todas partes de el mundo..



En todas partes de el mundo..







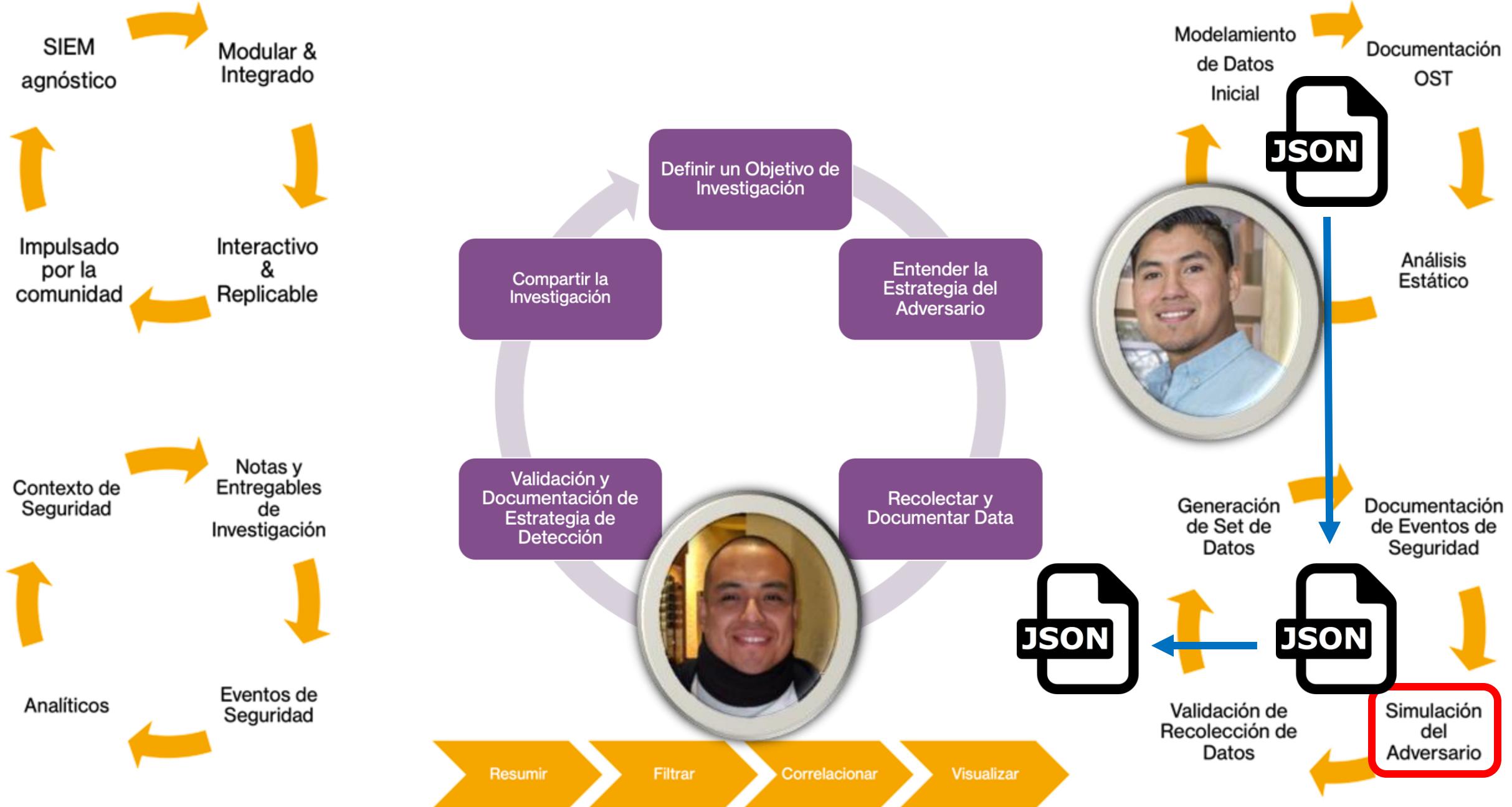
Bienvenidos a Mordor

Qué tal si unimos fuerzas, simulamos, coleccionamos data y la compartimos?

@Mordor_Project

- Eventos de seguridad pre-grabados, generados a través de la simulación de técnicas usadas por adversarios en
- Formato JavaScript Object Notation (**JSON**)
- Sets de datos categorizados por plataformas, grupos de adversarios, tácticas y técnicas definidas por MITRE - ATT&CK
- Datasets pequeñas y grandes





<https://mordordatasets.com>



The Mordor Project

Q Search this book...

MORDOR ENVIRONMENTS

The Shire
Erebor

HOW TO

Create 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 DCOM ShellWindows
WMIC Add User Backdoor
WMI Event Subscription
Empire Invoke PsExec
Empire Invoke Msbuild
Empire Launcher VBS
Covenant InstallUtil



Windows

ATT&CK Navigator View

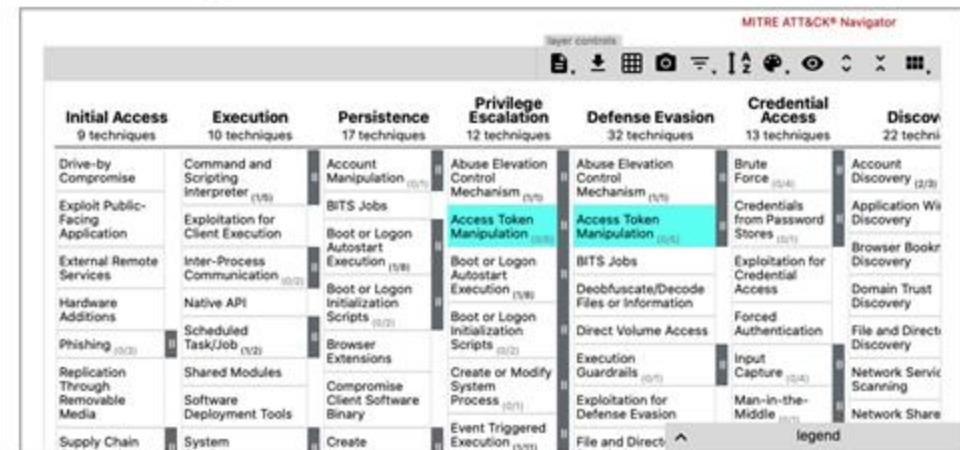


Table View

Created	Dataset	Description
2020/08/05	Covenant DCSync	This dataset represents adversaries with enough permissions (domain admin) adding an ACL to the Root Domain for any user, despite being in no privileged groups, having no malicious sidHistory, and not having local admin rights on the domain controller itself.

Técnicas específicas
(Small datasets)

Varias técnicas
relacionadas
(Large datasets)

SCM and DLL Hijack IKEEXT

Persistence

- Empire Userland Registry Run Key
- Empire Userland Scheduled Tasks
- Empire Elevated WMI Subscription
- Empire Elevated Scheduled Tasks
- SCM and DLL Hijacking IKEEXT**
- Empire Elevated Registry
- Privilege Escalation
- Empire UAC Shell API FodHelper
- Empire Invoke Runas
- Empire Elevated WMI Subscription
- Empire DLL Injection
- Empire PSInject
- SCM and DLL Hijacking IKEEXT
- Defense Evasion
- Covenant Grunt Msbuild
- Empire Wdigest Downgrade
- Empire Enabling RDP
- Empire Invoke Runas
- Empire Mimikatz OPTH
- Empire DLL Injection
- Empire Launcher SCT Regsvr32
- Empire PSInject
- SCM and DLL Hijacking IKEEXT
- Empire Invoke Msbuild
- Empire DCSync ACL
- Extended NetNTLM Downgrade
- Covenant InstallUtil
- Credential Access



Contents

Metadata

Dataset Description

Adversary View

Explore Mordor Dataset

Adversary View

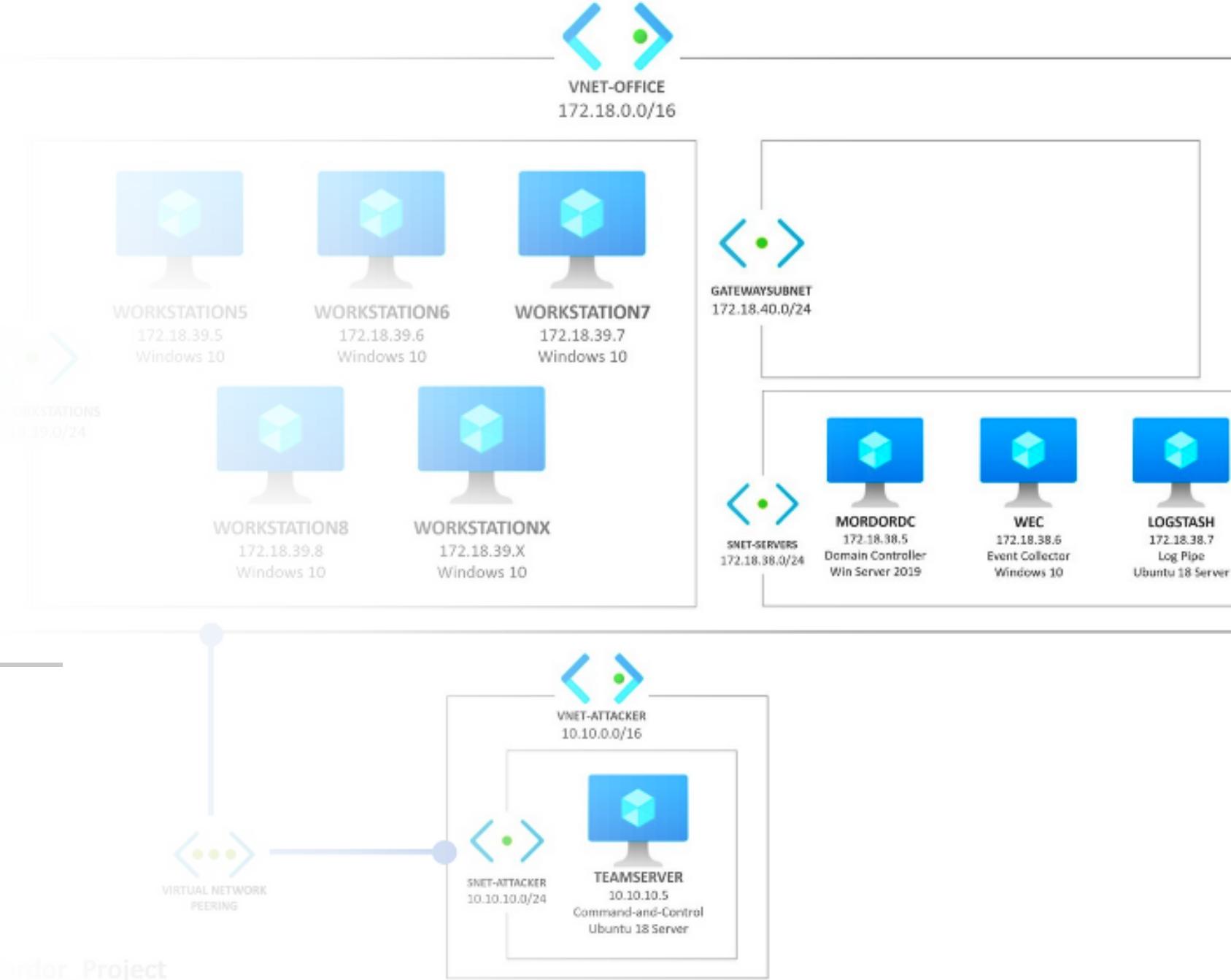
```
(Empire: NZB6SE34) > upload /tmp/wlbsctrl.dll
[*] Tasked agent to upload wlbsctrl.dll, 124 KB
[*] Tasked NZB6SE34 to run TASK_UPLOAD
[*] Agent NZB6SE34 tasked with task ID 46
(Empire: NZB6SE34) > shell COPY .\wlbsctrl.dll \\HR001\C$\Windows\System32\wlbsctrl.dll
[*] Tasked NZB6SE34 to run TASK_SHELL
[*] Agent NZB6SE34 tasked with task ID 47
(Empire: NZB6SE34) > ..Command execution completed.

(Empire: NZB6SE34) > shell sc.exe `\\HR001 stop IKEEXT
[*] Tasked NZB6SE34 to run TASK_SHELL
[*] Agent NZB6SE34 tasked with task ID 48
(Empire: NZB6SE34) > SERVICE_NAME: IKEEXT
    TYPE          : 30  WIN32
    STATE         : 3  STOP_PENDING
                  (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE  : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0x1388
..Command execution completed.

(Empire: NZB6SE34) > shell sc.exe `\\HR001 query IKEEXT
[*] Tasked NZB6SE34 to run TASK_SHELL
[*] Agent NZB6SE34 tasked with task ID 49
(Empire: NZB6SE34) > SERVICE_NAME: IKEEXT
    TYPE          : 20  WIN32_SHARE_PROCESS
    STATE         : 1  STOPPED
    WIN32_EXIT_CODE  : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT     : 0x0
    WAIT_HINT      : 0x0
..Command execution completed.
```



Diseño de Ambientes de Prueba

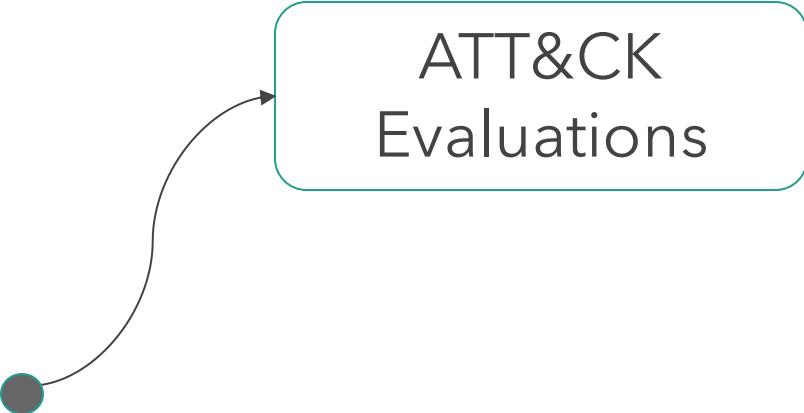


Usando el Proyecto SimuLand



- **Cloud templates y scripts:**
 - Simulación de adversarios
 - Generación-recolección de datos
 - Enfocado en el aprendizaje de la estrategia del adversario desde una perspectiva de datos.
- **Múltiples ambientes modulares** que permiten la adaptación de requerimientos específicos de un tema específico (research).
- <https://github.com/OTRF/SimuLand>

Ambientes: ATT&CK Evaluations



APT29 Evaluations

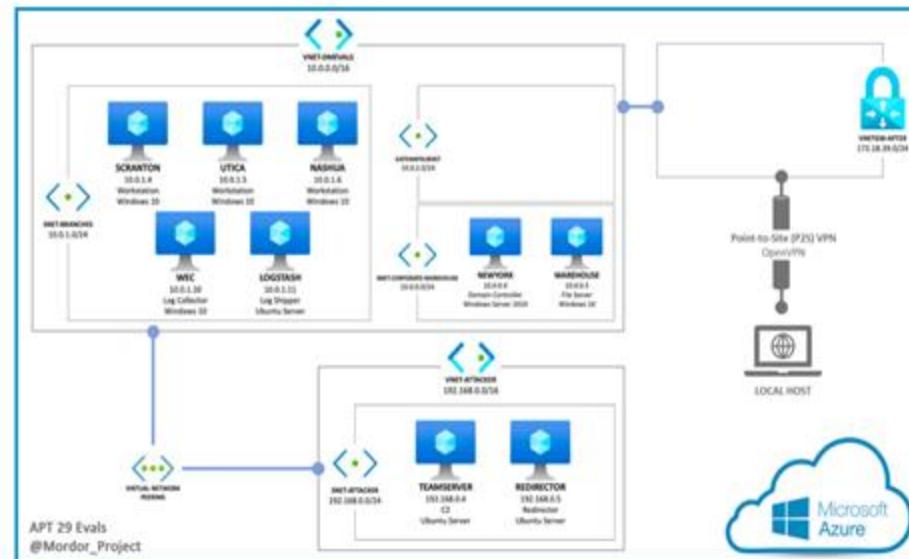
[Deploy to Azure](#) [Visualize](#)

This Mordor environment was built to replicate a similar setup developed by the ATT&CK Evals team following their official [emulation plan](#) methodology and using several of the [PowerShell scripts](#) used for the main evaluation. The main goal of this environment is to share the free telemetry produced after executing the APT29 emulation plan scenarios and create detection research opportunities for the Infosec community.

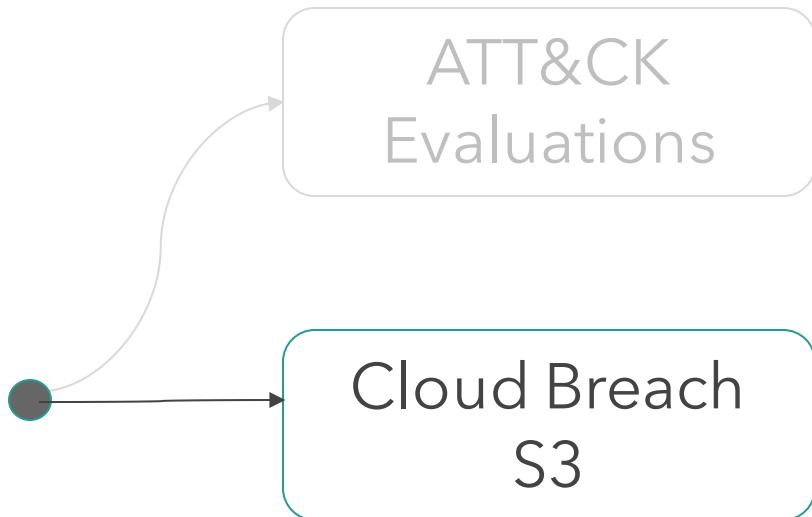
Blog Post

<https://medium.com/threat-OTRF/mordor-labs-part-1-deploying-att-ck-apt29-evals-environments-via-arm-templates-to-create-1c6c4bc32c9a>

Network Design



Ambientes: Cloud Breach S3



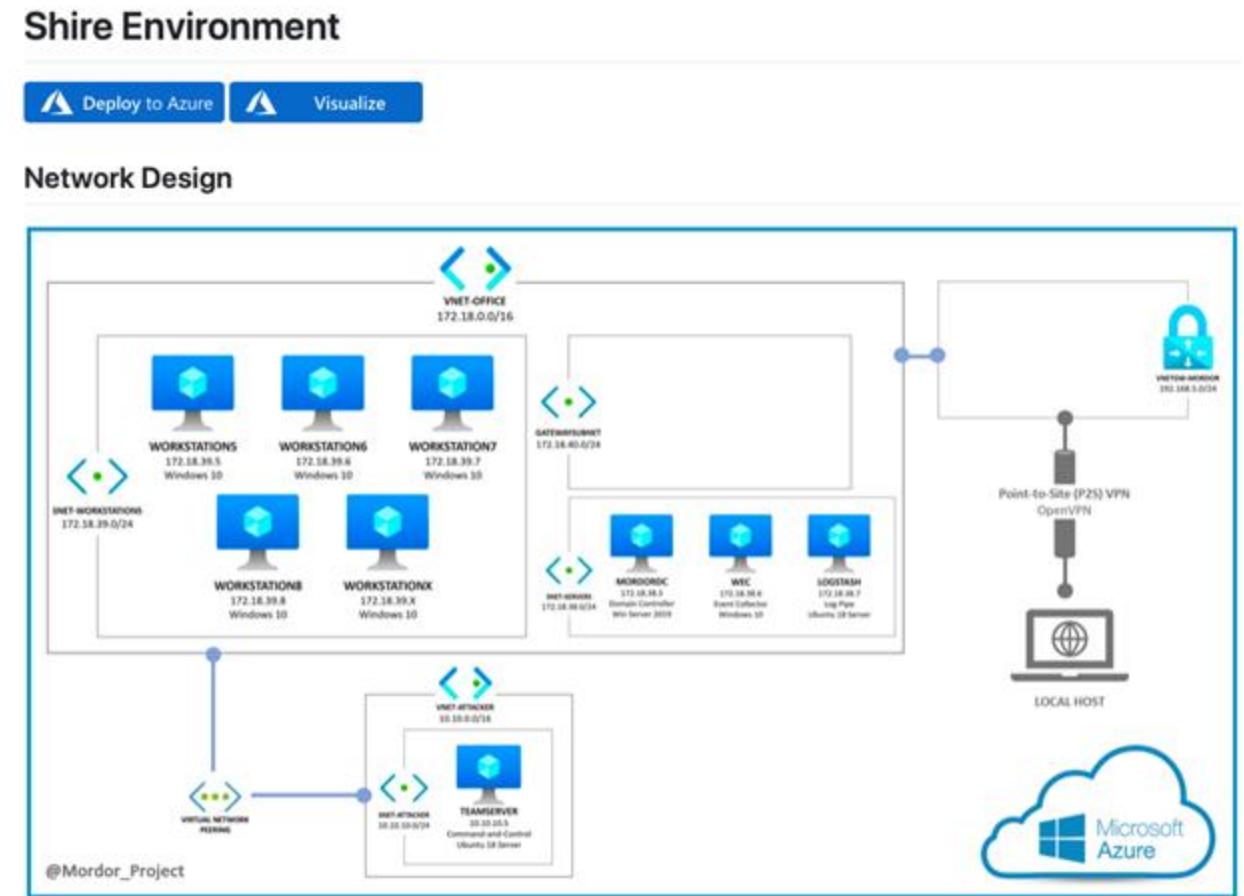
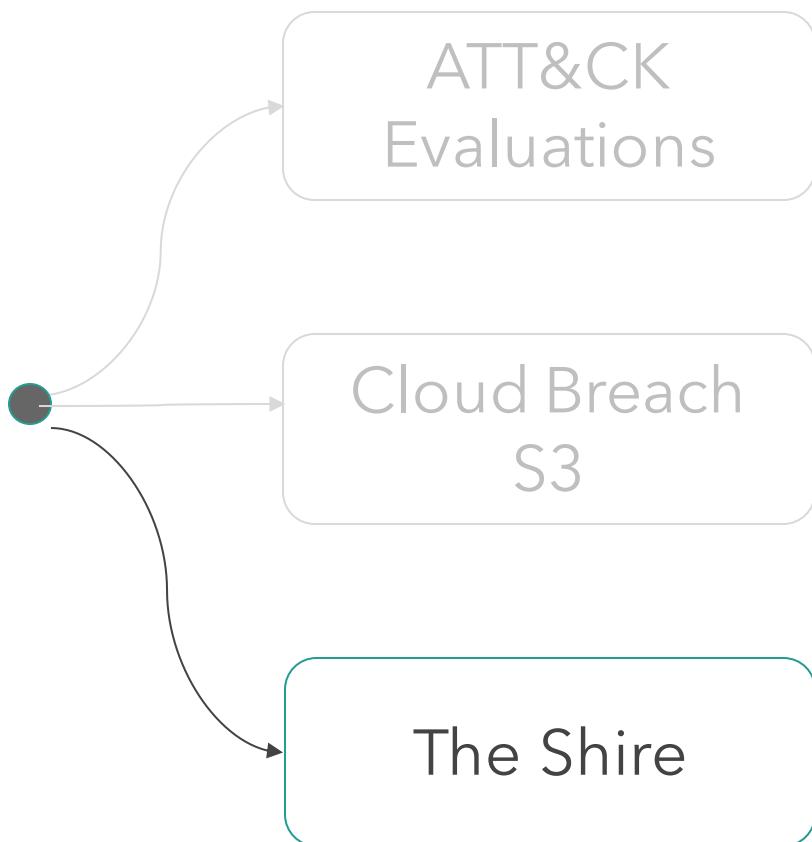
Cloud Breach S3

An environment to replicate an adversary abusing a misconfigured EC2 reverse proxy to obtain instance profile keys (Access and Secret) and eventually exfiltrate files from an S3 bucket. The configurations and deployment templates were adapted from the [Rhino Security labs - Cloud Goat project](#). The automatic cloudtrail configurations and templates were added to the environment with the main goal to extract the logs and share the dataset with the InfoSec community via the [Mordor project](#).

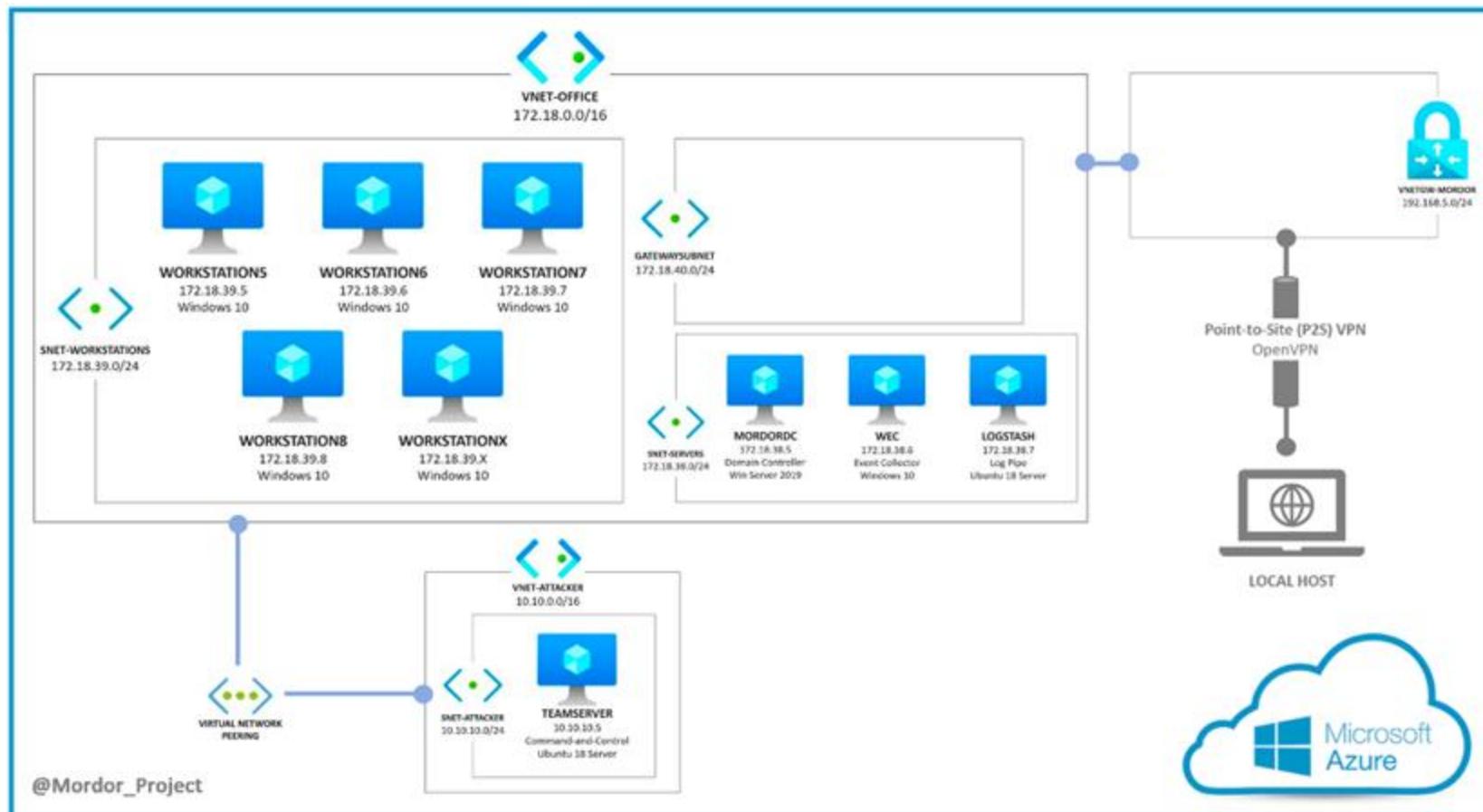
Resources Deployed

- S3 bucket (Sensitive Data)
 - One file uploaded at deployment time
- EC2
 - Nginx Installed (Reverse Proxy)
 - BankingWAFRole IAM Role
 - Full Access to S3 Bucket
- CloudTrail Trail
 - GlobalS3DataEventsTrail
 - Data Resource: S3 Bucket
 - API & Management Events
- S3 Bucket (CloudTrail)
- EC2 (Log Collector)
 - Logstash
 - S3 Input Plugin
 - Kafka Output Plugin
 - Kafka Docker Container
 - Topic: clouptrail
 - Kafkacat
 - Ready to consume logs from kafka

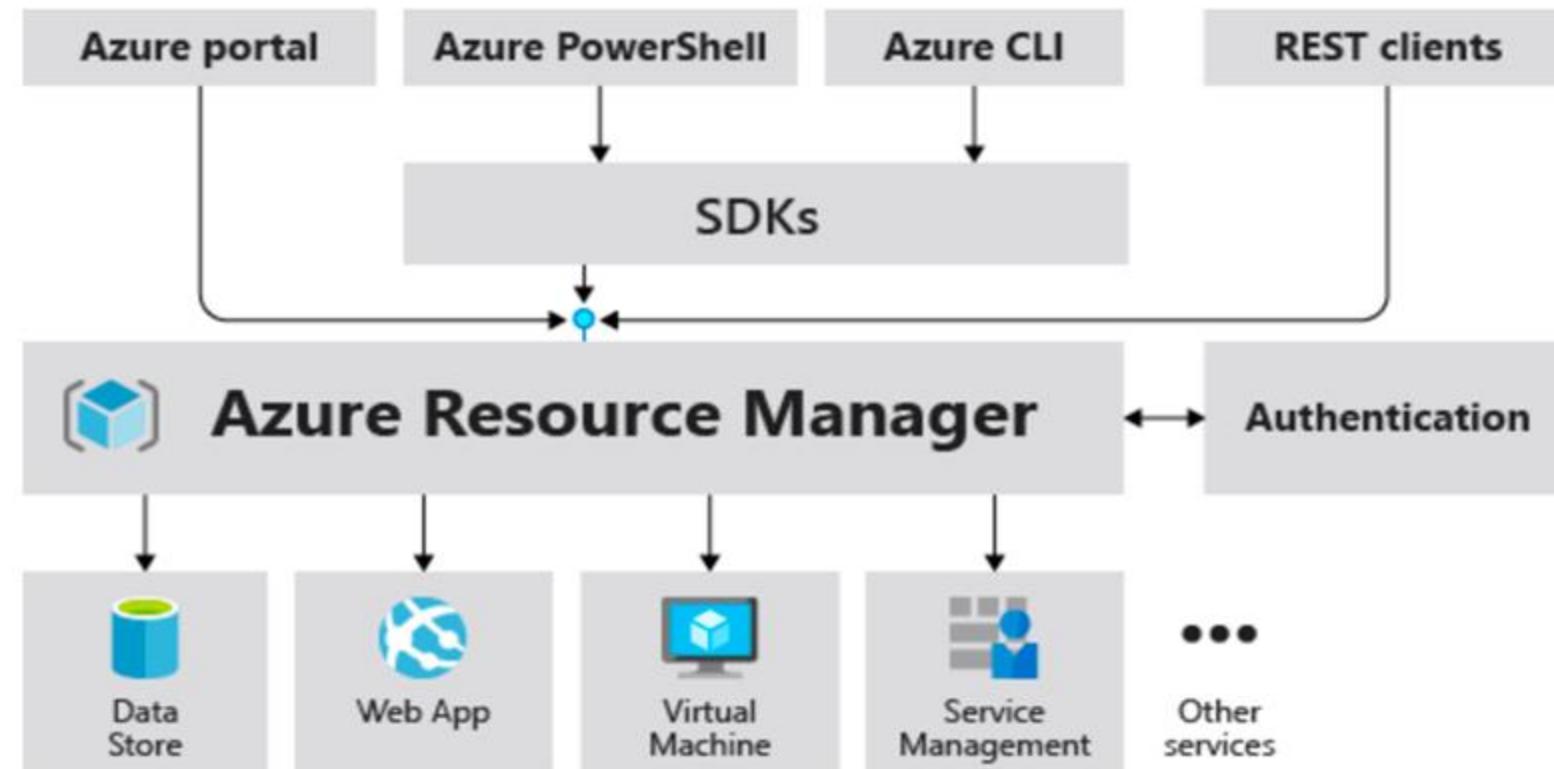
Ambientes: The Shire



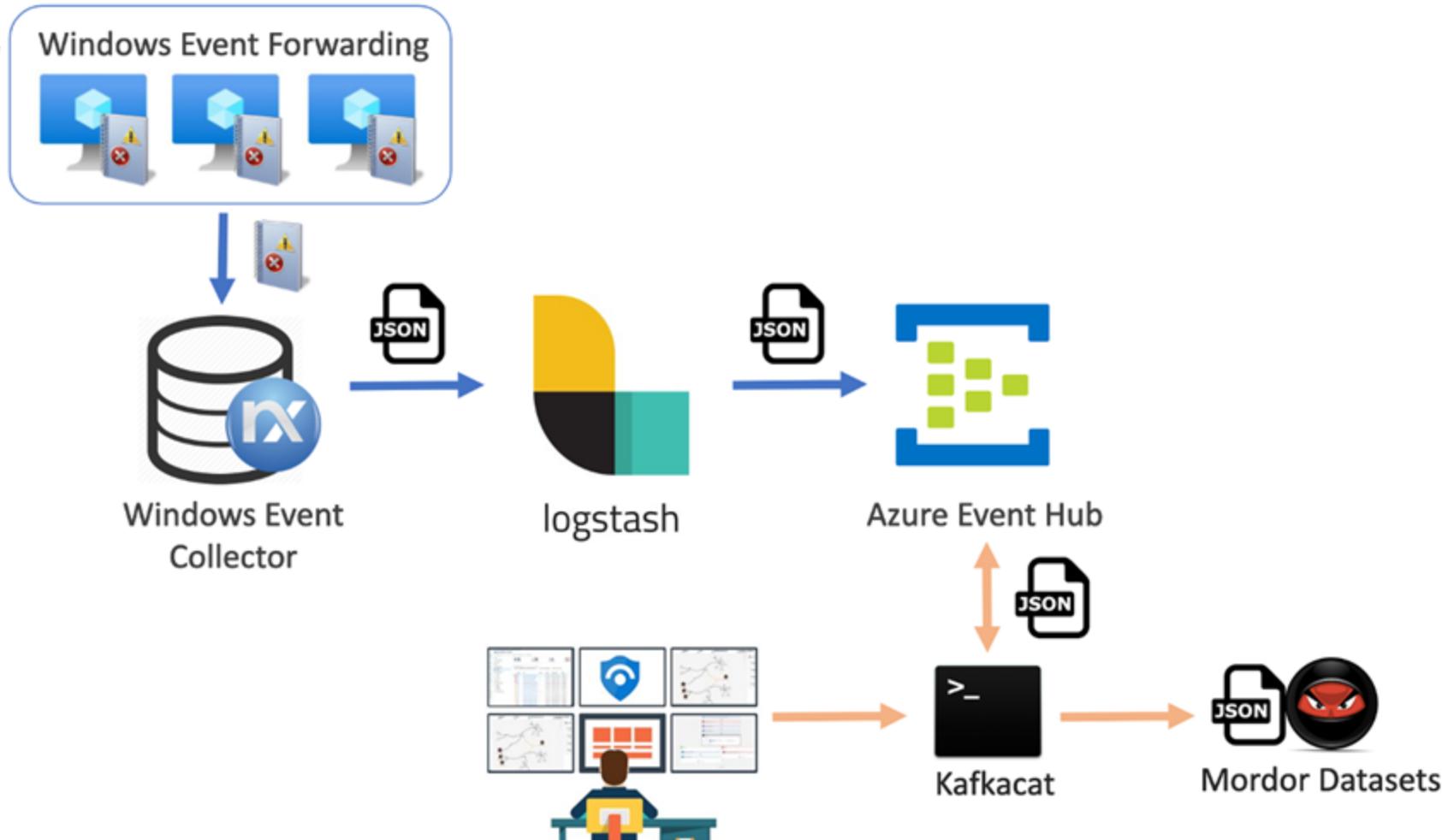
The Shire (Windows)



Servicio de Azure Resource Manager



Coleccionando Data!



<https://github.com/OTRF>

Blacksmith

[OTRF / Blacksmith](#)

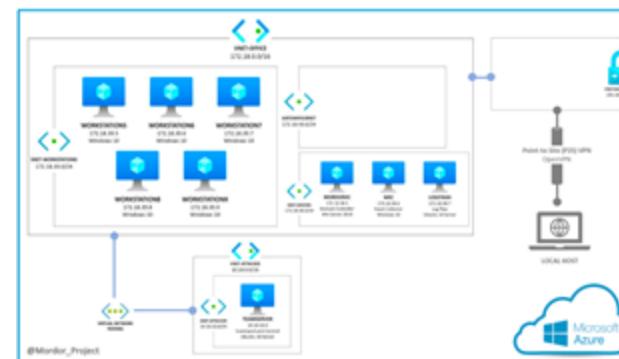
Code Issues Pull requests Actions Projects Wiki Security

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

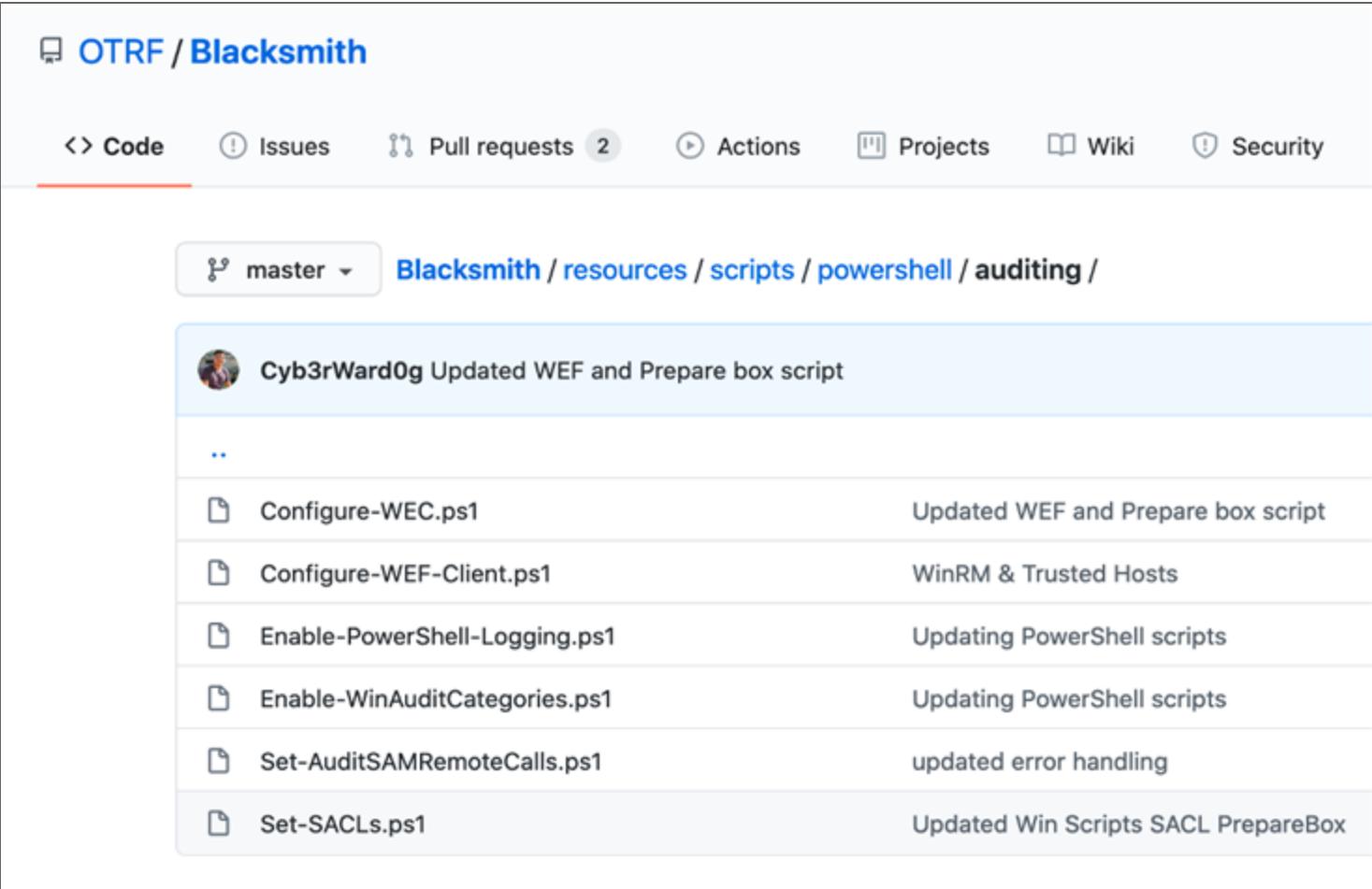
SimuLand



Mordor



Configurando Sistemas y Auditoria de Eventos



The screenshot shows a GitHub repository named "OTRF / Blacksmith". The "Code" tab is selected, and the URL in the address bar is "Blacksmith / resources / scripts / powershell / auditing /". A dropdown menu shows "master" is selected. Below the header, there is a commit message from "Cyb3rWard0g" that says "Updated WEF and Prepare box script". The commit details a list of PowerShell scripts and their descriptions:

File	Description
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

Configurando PowerShell Logging

21 lines (19 sloc) | 918 Bytes

```
1 # Author: Roberto Rodriguez (@Cyb3rWard0g)
2 # License: GPL-3.0
3
4 # Enable PowerShell Logging
5 $regConfig = @"
6 regKey,name,value,type
7 "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging","EnableScriptBlockLogging",1,"DWORD"
8 "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging","EnableScriptBlockInvocationLogging",1,"DWORD"
9 "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging","EnableModuleLogging",1,"DWORD"
10 "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames",*,*,,"String"
11 "@
12
13 Write-host "Setting up PowerShell registry settings.."
14 $regConfig | ConvertFrom-Csv | ForEach-Object {
15     if(!(Test-Path $_.regKey)){
16         Write-Host $_.regKey " does not exist.."
17         New-Item $_.regKey -Force
18     }
19     Write-Host "Setting " $_.regKey
20     New-ItemProperty -Path $_.regKey -Name $_.name -Value $_.value -PropertyType $_.type -force
21 }
```

Reglas de Auditoria para el Registro

```
30 "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\JD";"Everyone";"QueryValues";"None";"None";"Success"
31 "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Skew1";"Everyone";"QueryValues";"None";"None";"Success"
32 "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\GBG";"Everyone";"QueryValues";"None";"None";"Success"
33 "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Data";"Everyone";"QueryValues";"None";"None";"Success"
34 "@
35
36 write-host "Enabling audit rules.."
37 $AuditRules | ConvertFrom-Csv -Delimiter ';' | ForEach-Object {
38     if(!(Test-Path $_.regKey)){
39         Write-Host $_.regKey " does not exist.."
40     }
41     else {
42         Write-Host "Updating SACL of " $_.regKey
43         Set-AuditRule -RegistryPath $_.regKey -IdentityReference $_.identityReference -Rights $_.rights.split(",")
44     }
45 }
```

Reglas de Auditoria para Servicios



```
68 $ServiceRules = @"
69 service;addition
70 "IKEEXT";"(AU;SAFA;RPWPDTCCCLC;;;WD)"
71 "SessionEnv";"S:(AU;SAFA;RPWPDTCCCLC;;;WD)"
72 "scmanager";"(AU;SAFA;GA;;;NU)"
73 "@
74
75 $ServiceRules | ConvertFrom-Csv -Delimiter ';' | ForEach-Object {
76     if(Get-Service $service){
77         Write-Host "[+] Processing " $_.service
78         # Get Sddl
79         $sddl = (& $env:SystemRoot\System32\sc.exe sdshow $_.service | Out-String).Trim()
80         # Define new Sddl
81         $newSddl = ('{0}{1}' -f $sddl, $_.addition).Trim()
82         # Update Sddl
83         write-host "  [>] Updating SDDL.."
84         & $env:SystemRoot\System32\sc.exe sdset $_.service "$newSddl"
85     }
86 }
```

Reglas de Auditoria para Servicios



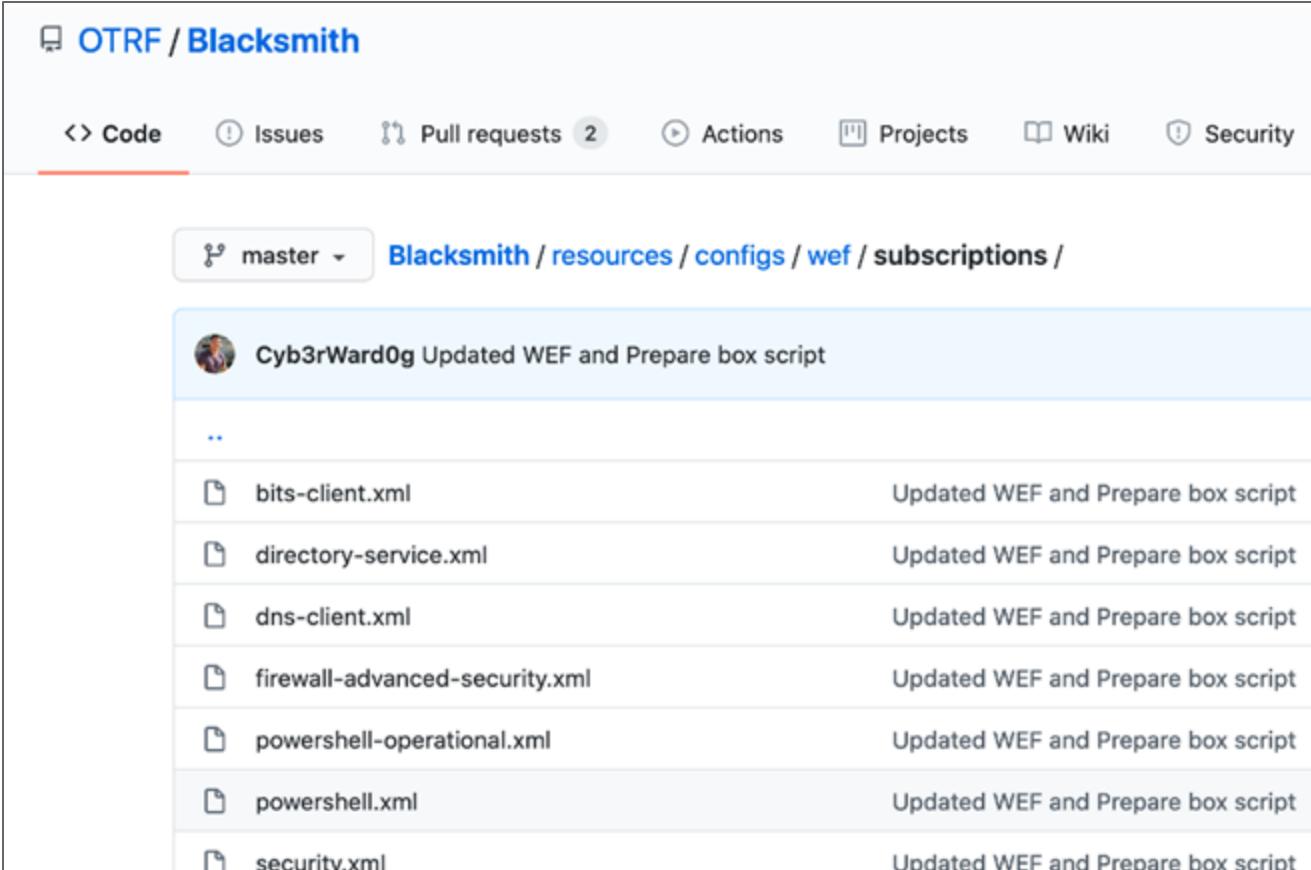
```
68 $ServiceRules = @"
69 service;addition
70 "IKEEXT";"(AU;SAFA;RPWPDTCCCLC;;;WD)"
71 "SessionEnv";"S:(AU;SAFA;RPWPDTCCCLC;;;WD)"
72 "scmanager";"(AU;SAFA;GA;;;NU)"
73 "@
74
75 $ServiceRules | ConvertFrom-Csv -Delimiter ';' | ForEach-Object {
76     if(Get-Service $service){
77         Write-Host "[+] Processing " $_.service
78         # Get Sddl
79         $sddl = (& $env:SystemRoot\System32\sc.exe sdshow $_.service | Out-String).Trim()
80         # Define new Sddl
81         $newSddl = ('{0}{1}' -f $sddl, $_.addition).Trim()
82         # Update Sddl
83         write-host "  [>] Updating SDDL.."
84         & $env:SystemRoot\System32\sc.exe sdset $_.service "$newSddl"
85     }
86 }
```

AU;SAFA;RPWPDTCCCLC;;;;WD



```
51 Ace Type:  
52 "AU": SYSTEM_AUDIT_ACE_TYPE  
53 Ace Flags:  
54 "SA"    : SUCCESSFUL_ACCESS_ACE_FLAG  
55 "FA"    : FAILED_ACCESS_ACE_FLAG  
56 Rights:  
57 RP : SERVICE_START – start the service  
58 WP: SERVICE_STOP – stop the service  
59 DT: SERVICE_PAUSE_CONTINUE – pause / continue the service  
60 CC – SERVICE_QUERY_CONFIG – ask the SCM for the service's current configuration  
61 LC – SERVICE_QUERY_STATUS – ask the SCM for the service's current status  
62 Object Guid: NA  
63 Inherit Object Guid: NA  
64 Account SIDs:  
65     * WD: SDDL_EVERYONE  
66     * NU: SDDL_NETWORK  
67 #>
```

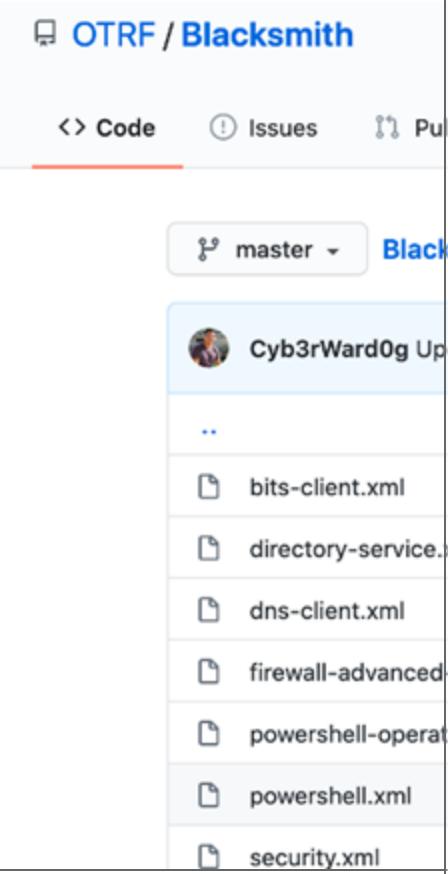
Windows Event Forwarding (WEF)



The screenshot shows a GitHub repository interface for the 'OTRF / Blacksmith' project. The 'Code' tab is selected, and the URL in the address bar is `Blacksmith / resources / configs / wef / subscriptions /`. A dropdown menu shows 'master'. Below the navigation bar, a commit by 'Cyb3rWard0g' is listed: 'Updated WEF and Prepare box script'. The commit message also includes '..'. Below the commit, there is a list of XML files and their descriptions:

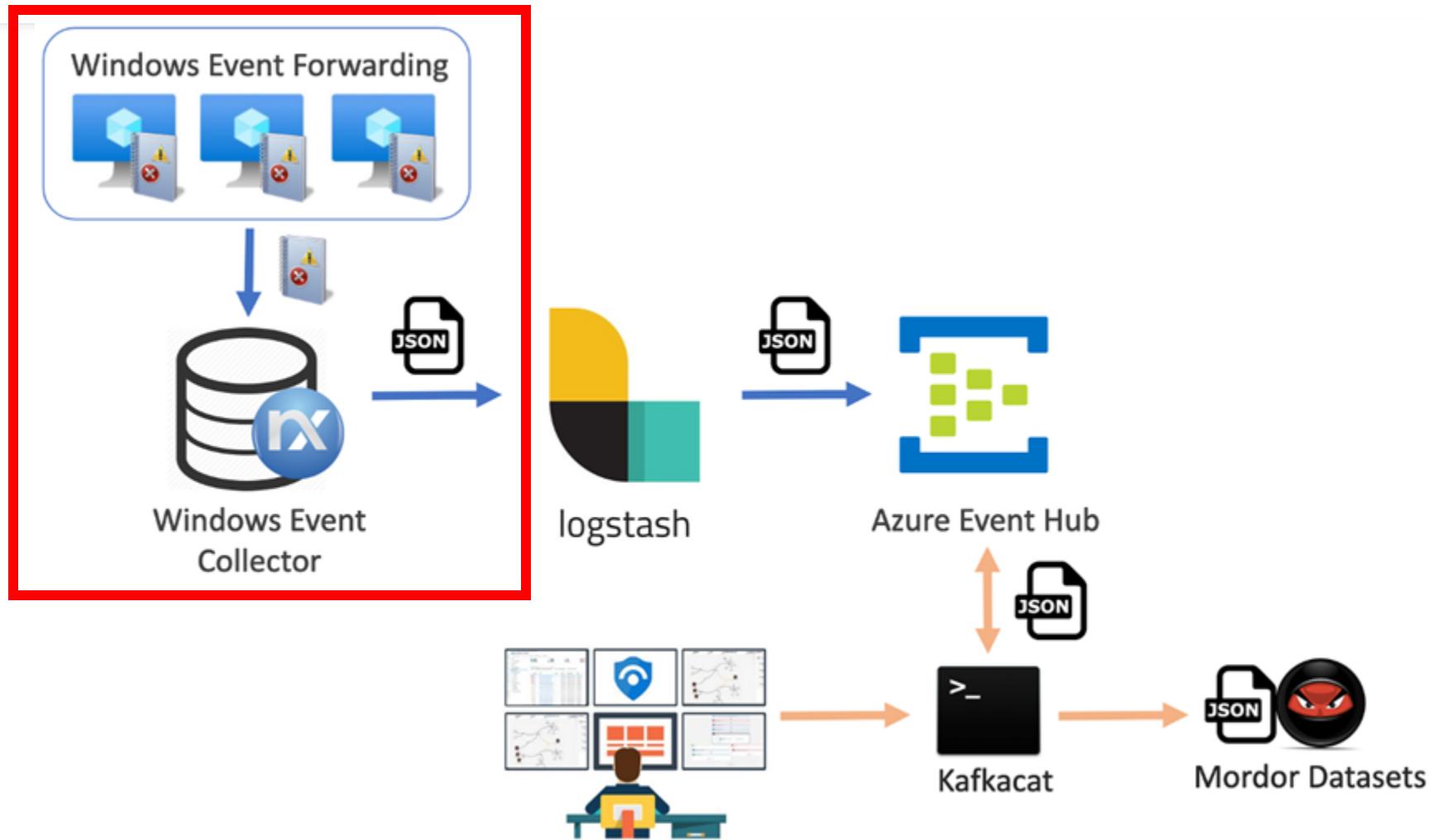
File	Description
bits-client.xml	Updated WEF and Prepare box script
directory-service.xml	Updated WEF and Prepare box script
dns-client.xml	Updated WEF and Prepare box script
firewall-advanced-security.xml	Updated WEF and Prepare box script
powershell-operational.xml	Updated WEF and Prepare box script
powershell.xml	Updated WEF and Prepare box script
security.xml	Updated WEF and Prepare box script

Windows Event Forwarding (WEF)

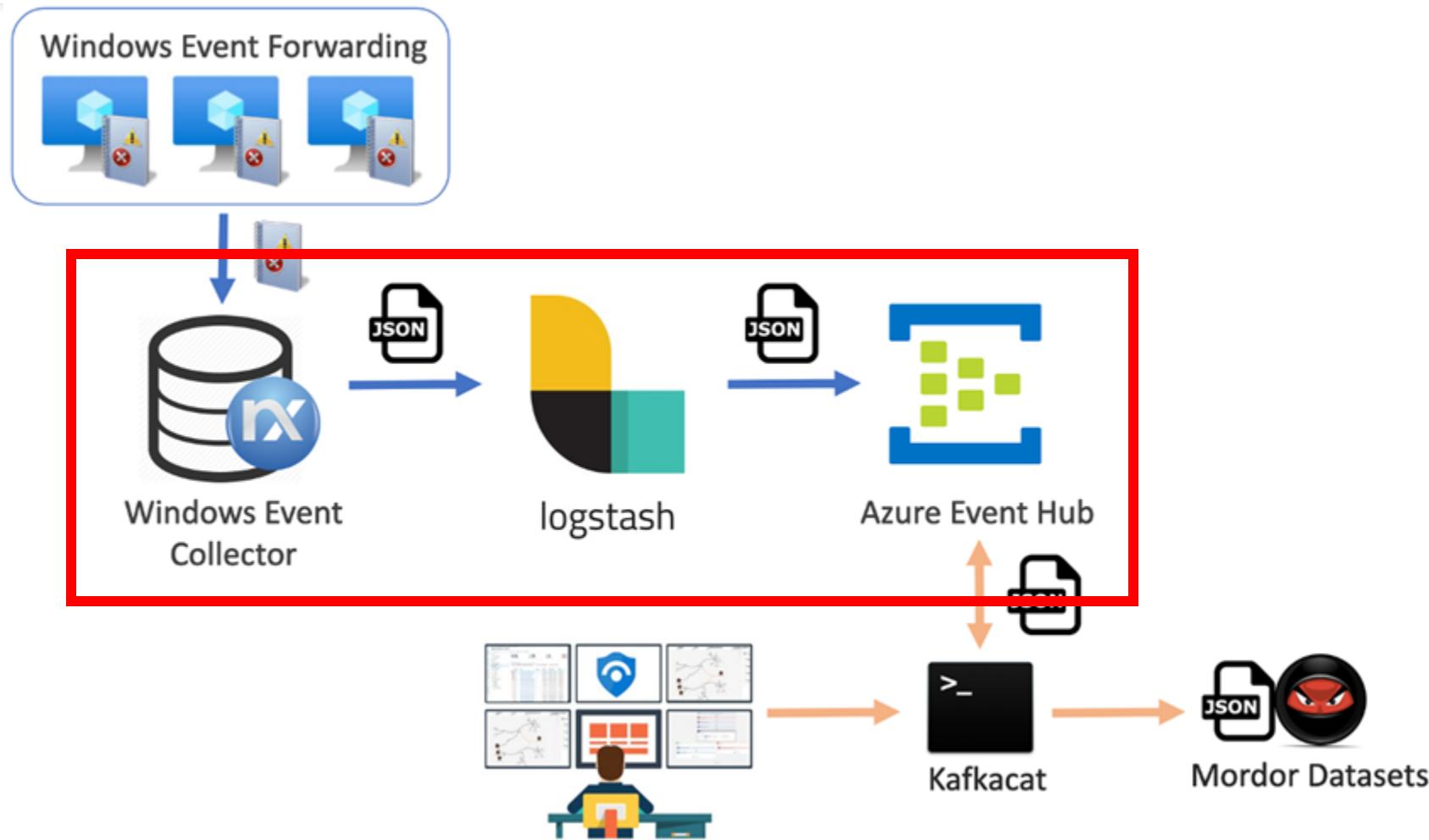


```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
<SubscriptionId>Sysmon</SubscriptionId>
<SubscriptionType>SourceInitiated</SubscriptionType>
<Description>Everything from the Microsoft-Windows-Sysmon/Operational channel</Description>
<Enabled>true</Enabled>
<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:NSG:BAD:P(A;;GA;;;DC)(A;;GA;;;DD)S:</AllowedSourceDomainComputers>
</Subscription>
```

Todavia ni enviamos data..



NxLog (CE) -> Logstash -> Azure Event Hubs



Azure Event Hub

Home > evhns-MORDORi3sgm6cljcxza

Event Hubs Namespace

Search (Cmd+ /) Event Hub Delete Refresh

Overview Host name: evhns-MORDORi3sgm6cljcxza.servicebus.windows.net

Activity log Tags (change): Click here to add tags

Access control (IAM)

Tags

Diagnose and solve problems

Events

1 EVENT HUB KAFKA SURFACE ENABLED

Show metrics: Requests Messages Throughput

For the last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

50k
45k
40k
35k
30k
25k
20k
15k
10k
5k
0

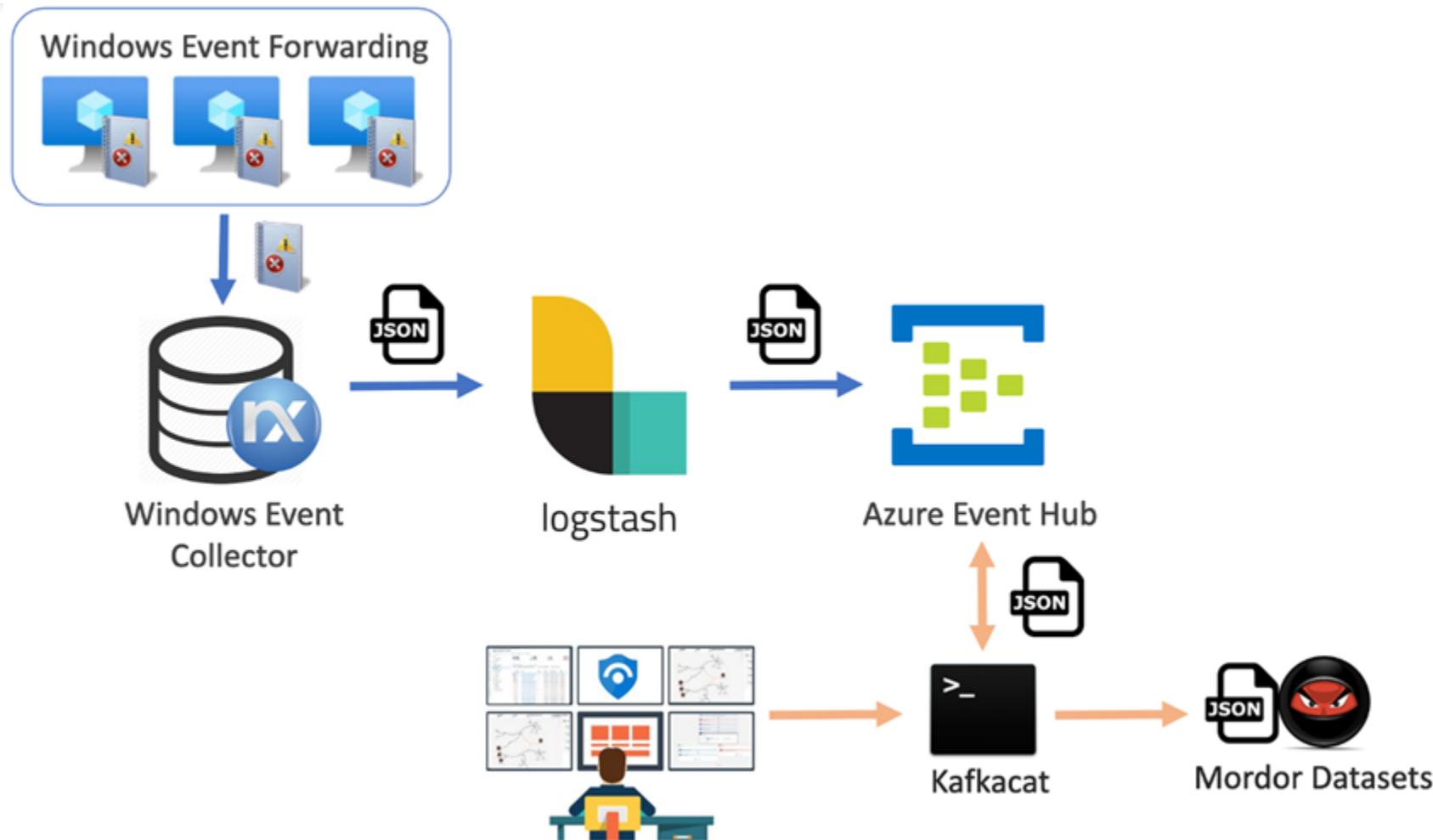
11:15 PM Sep 2 11:31 PM 11:45 PM Sep 3

Incoming Messages (Sum): evhns-mordor3sgm6cljcxza 6.64k Outgoing Messages (Sum): evhns-mordor3sgm6cljcxza 0 Captured Messages (Sum): evhns-mordor3sgm6cljcxza 0 Capture Backlog (Sum): evhns-mordor3sgm6cljcxza 0

Search to filter items...

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

Azure Event Hubs + Kafkacat



Azure Event Hubs + Kafkacat

- **kafkacat** es un productor y consumidor, generico y no-JVM, para Apache Kafka ≥ 0.8 , se puede pensar como un netcat para Kafka.
- En modo **productor**, kafkacat lee mensajes y los envía al cluster (-b), tópico (-t) y partición (-p) de Azure Event Hub.
- En modo **consumidor**, Kafkacat lee los mensajes que se encuentran en un tópico y partición en Azure Event Hub y los escribe al terminal o a un file.

Kafkacat: Modo Consumidor

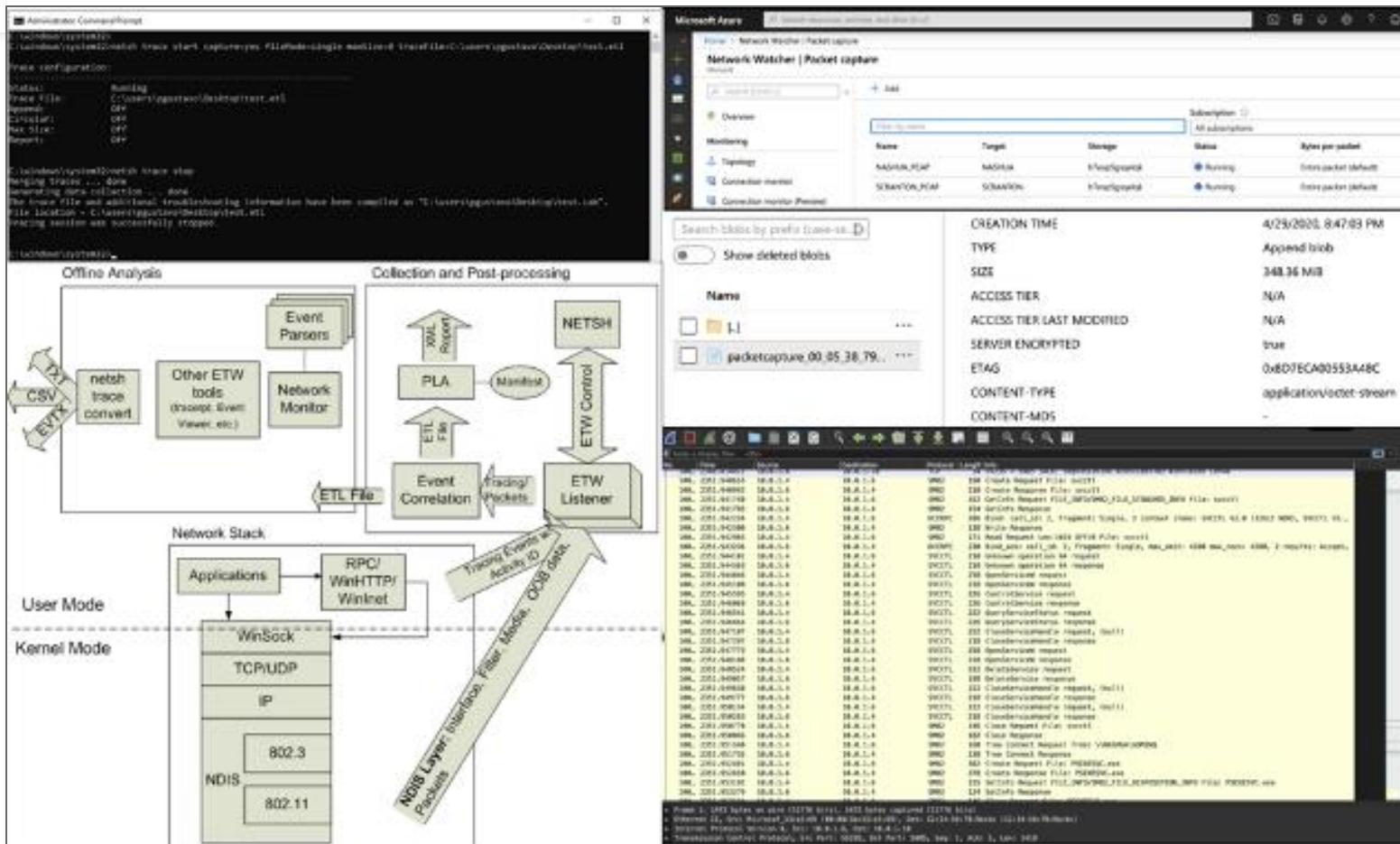
```
kafkacat -b <AzureEventHub>:9093 -t  
evh-mordor -F kafkacat.conf -C -o end
```

Kafkacat: Modo Consumidor

Kafkacat: Modo Consumidor

Workstation Inventory - 2023-01-01							
Name	IP Address	Machine Name	Manufacturer	Processor	FPS	Display	Last Sync
KYLLOKONNEN	192.168.1.5	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
YOSILKINEN	192.168.1.6	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
UROKKIVAA	192.168.1.7	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
Detailed Agent Status							
Name	IP Address	Machine Name	Manufacturer	Processor	FPS	Display	Last Sync
KYLLOKONNEN	192.168.1.5	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
YOSILKINEN	192.168.1.6	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
UROKKIVAA	192.168.1.7	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
Detailed Agent Status							
Name	IP Address	Machine Name	Manufacturer	Processor	FPS	Display	Last Sync
KYLLOKONNEN	192.168.1.5	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
YOSILKINEN	192.168.1.6	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
UROKKIVAA	192.168.1.7	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
Detailed Agent Status							
Name	IP Address	Machine Name	Manufacturer	Processor	FPS	Display	Last Sync
KYLLOKONNEN	192.168.1.5	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
YOSILKINEN	192.168.1.6	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00
UROKKIVAA	192.168.1.7	WORKSTATION	ASUS ROG Strix G17	Intel Core i9-13900K	7500	QHD	2023-01-01 10:00:00

Y tambien capuras trafico de el network?



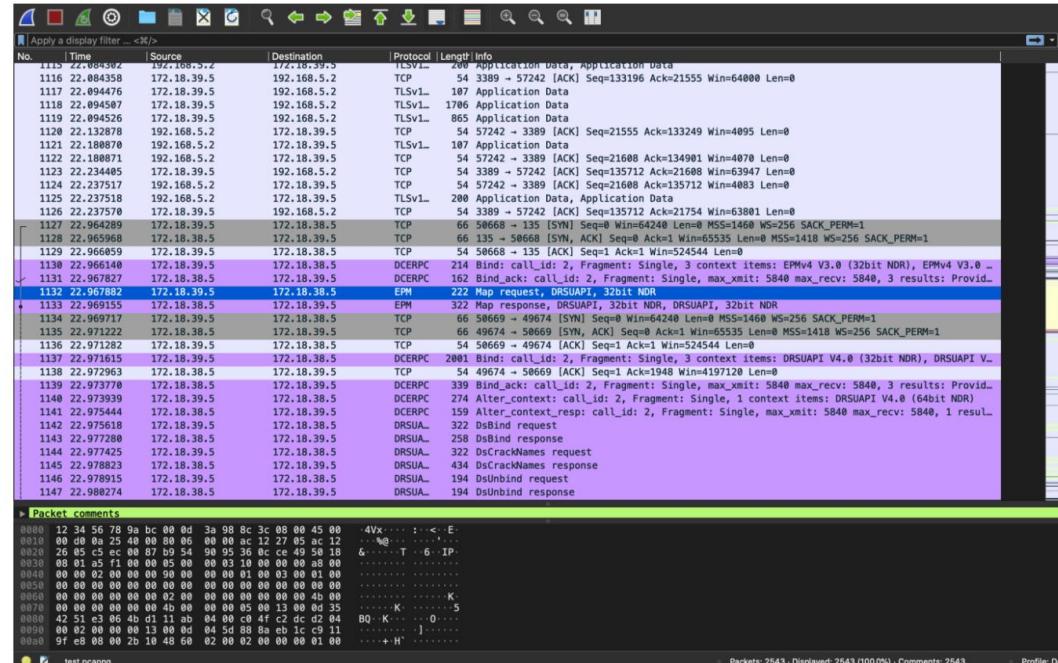
Network Shell (Windows ETW)

```
C:\> netsh trace start capture=yes fileMode=single maxSize=0  
traceFile=C:\users\pgustavo\Desktop\test.etl
```

- **capture:** Specifies whether packet capture is enabled.
- **fileMode:** File mode applied when tracing output is generated.
- **maxSize:** Maximum size in MB for saved trace file. 0=No Max.
- **traceFile:** Location and name of the .etl output file.

ETL2PCAPNG

```
etl2pcapng.exe test.etl test.pcapng
```



Azure Network Watcher (PCAPs)

```
az network watcher packet-capture create --resource-group
${RESOURCE_GROUP} --vm ${COMPUTER} --name "${COMPUTER}_PCAP"
--storage-account ${STORAGE_ACCOUNT} --filters "
[
{
  \"localIPAddress\": \"10.0.0.0-10.0.1.9\",
  \"remoteIPAddress\": \"10.0.0.0-10.0.1.9\"
},
{
  \"localIPAddress\": \"10.0.0.0-10.0.1.9\",
  \"remoteIPAddress\": \"192.168.0.0-192.168.0.10\"
}
]"
```

Azure Network Watcher (PCAPs)

The screenshot shows the Microsoft Azure Network Watcher | Packet capture interface. On the left, there's a navigation sidebar with icons for Overview, Monitoring (Topology, Connection monitor, Connection monitor (Preview)), and a search bar. The main area has a search bar at the top and a table listing two PCAP configurations:

Name	Target	Storage	Status	Bytes per packet
NASHUA_PCAP	NASHUA	h7eop5gsqelqk	Running	Entire packet (default)
SCRANTON_PCAP	SCRANTON	h7eop5gsqelqk	Running	Entire packet (default)

Below this, there's a blob storage section with a search bar, a 'Show deleted blobs' toggle, and a list of blobs. One blob is selected: 'packetcapture_00_05_38_79...'. To the right, detailed properties for this blob are shown:

CREATION TIME	4/29/2020, 8:47:03 PM
TYPE	Append blob
SIZE	348.36 MiB
ACCESS TIER	N/A
ACCESS TIER LAST MODIFIED	N/A
SERVER ENCRYPTED	true
ETAG	0x8D7ECA00553A48C
CONTENT-TYPE	application/octet-stream
CONTENT-MD5	-

Qué podemos hacer con la data?



Mordor Files

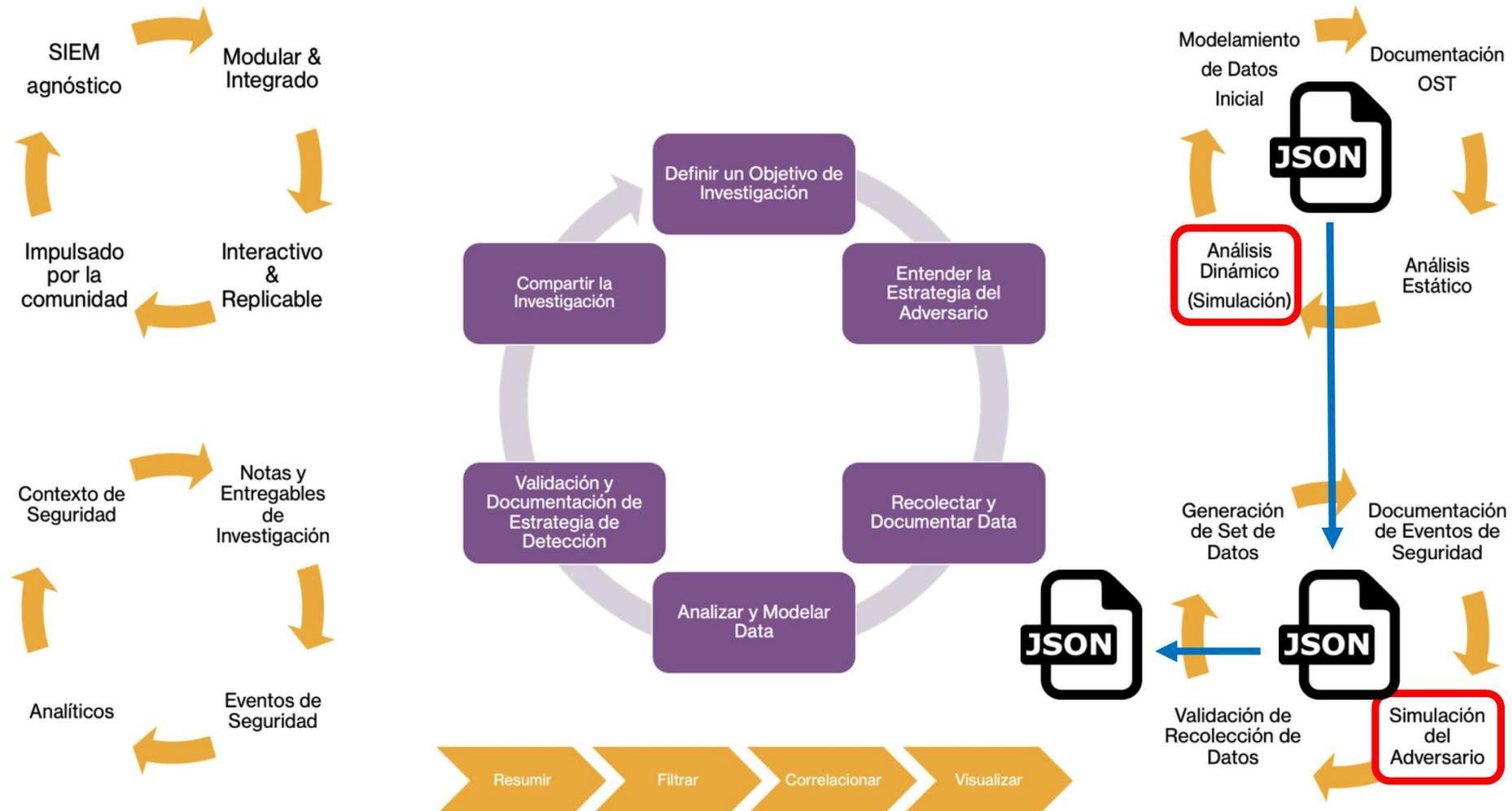
Entrenamiento de analistas de seguridad

Entrevistas de trabajo

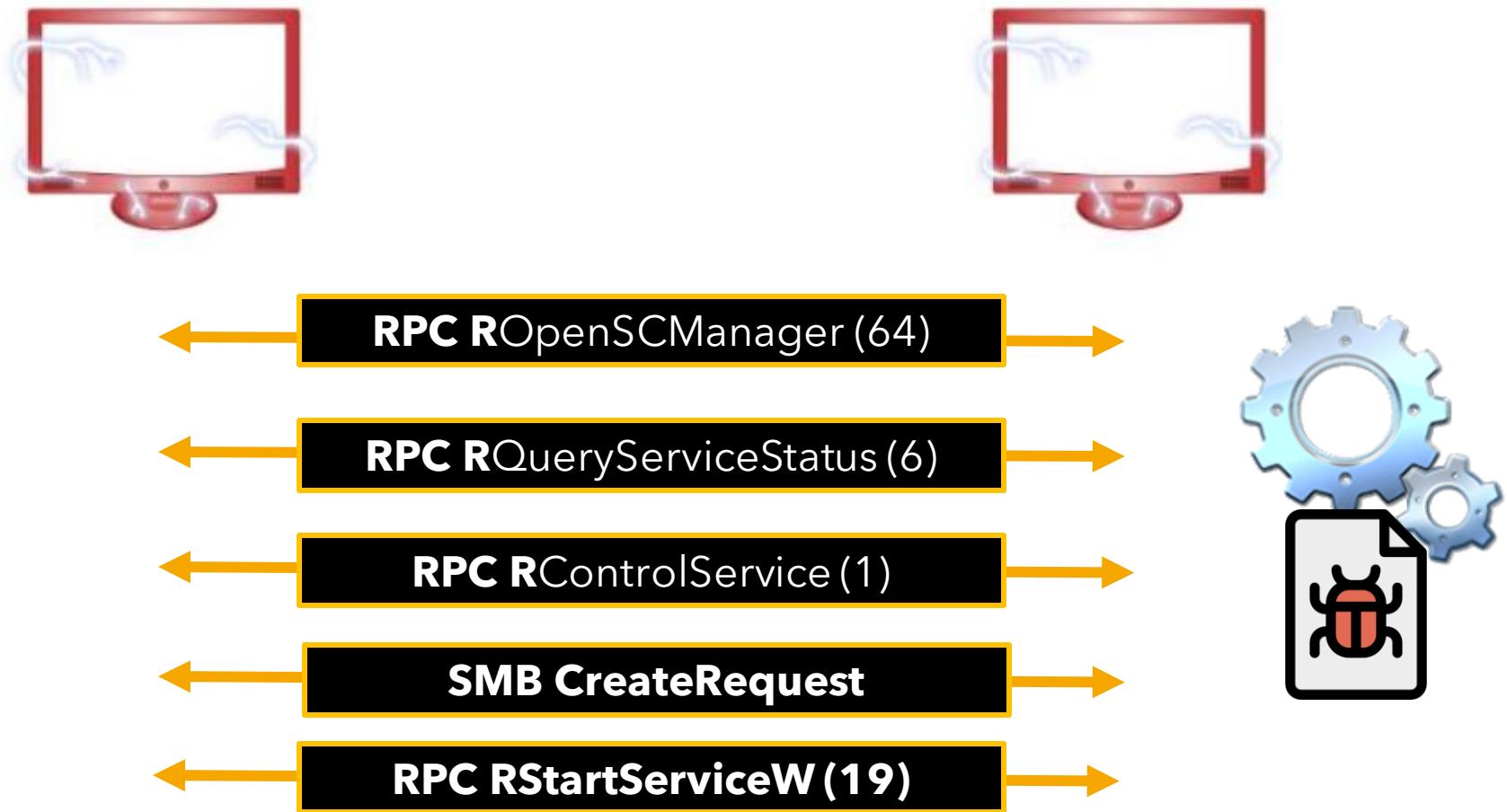
Eventos (Hackathons)

Validación de analíticos desarrollados in-house

Perspectiva R&D: Analyza y Modela Data



Abusando de el SCM y DLL Hijacks!



Ejemplo #1: SCM y DLL Hijack

```
scm_dll_hijack = spark.sql(  
    ...  
    SELECT Hostname, ObjectServer, AccessMask, a.IpAddress, a.TargetUserName  
    FROM dllhijack b  
    INNER JOIN (  
        SELECT TargetUserName, TargetLogonId, IpAddress  
        FROM dllhijack  
        WHERE LOWER(Channel) = 'security'  
        AND EventID = 4624 AND LogonType = 3 AND NOT TargetUserName LIKE "%$"  
    ) a  
    ON b.SubjectLogonId = a.TargetLogonId  
    WHERE LOWER(Channel) = 'security'  
    AND EventID = 4656 OR EventID = 4663  
    ...  
)  
scm_dll_hijack.show(truncate = False)
```

Hostname	ObjectServer	AccessMask	IpAddress	TargetUserName
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x20	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x4	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x14	172.18.39.5	pgustavo

Ejemplo #1: SCM y DLL Hijack

```
scm_dll_hijack = spark.sql(  
    ...  
    SELECT Hostname, ObjectServer, AccessMask, a.IpAddress, a.TargetUserName  
    FROM dllhijack b  
    INNER JOIN (  
        SELECT TargetUserName, TargetLogonId, IpAddress  
        FROM dllhijack  
        WHERE LOWER(Channel) = 'security'  
        AND EventID = 4624 AND LogonType = 3 AND NOT TargetUserName LIKE "%$"  
    ) a  
    ON b.SubjectLogonId = a.TargetLogonId  
    WHERE LOWER(Channel) = 'security'  
    AND EventID = 4656 OR EventID = 4663  
    ...)  
scm_dll_hijack.show(truncate = False)
```

- 0x1 - Conectar al Controlador de Servicio**
- 0x20 - Detiene el Servicio**
- 0x4 - Consulta Estado de el Service**
- 0x14 - Inicia el Servicio**

Hostname	ObjectServer	AccessMask	IpAddress	TargetUserName
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x20	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x4	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x1	172.18.39.5	pgustavo
WORKSTATION6.theshire.local	SC Manager	0x14	172.18.39.5	pgustavo

Ejemplo #2: Ejecución de Código via DCOM Excel RegisterXLL

```
network_logon_excel = spark.sql(  
    '''.  
        SELECT Hostname, Image, ImageLoaded, c.ParentCommandLine, c.CommandLine, c.IpAddress, c.TargetUserName  
        FROM mordorExcelXLL d  
        INNER JOIN (  
            SELECT ParentCommandLine, CommandLine, LogonId, a.IpAddress, a.TargetUserName, ProcessGuid  
            FROM mordorExcelXLL b  
            INNER JOIN (  
                SELECT TargetUserName, TargetLogonId, IpAddress  
                FROM mordorExcelXLL  
                WHERE LOWER(Channel) = 'security'  
                    AND EventID = 4624 AND LogonType = 3 AND NOT TargetUserName LIKE "%$"  
            ) a  
            ON b.LogonId = a.TargetLogonId  
            WHERE Channel = 'Microsoft-Windows-Sysmon/Operational'  
                AND EventID = 1  
                AND LOWER(CommandLine) LIKE '%excel%automation%'  
                AND LOWER(ParentCommandLine) LIKE '%dcomlaunch%'  
        ) c  
        ON d.ProcessGuid = c.ProcessGuid  
        WHERE Channel = 'Microsoft-Windows-Sysmon/Operational'  
            AND EventID = 7  
            AND LOWER(ImageLoaded) LIKE '%programdata%'  
    '''  
).show(truncate = False, vertical=True)  
  
-RECORD 0-  
Hostname | WORKSTATION6.theshire.local  
Image | C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE  
ImageLoaded | C:\ProgramData\calc.xll  
ParentCommandLine | C:\windows\system32\svchost.exe -k DcomLaunch -p  
CommandLine | "C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" /automation -Embedding  
IpAddress | 172.18.39.5  
TargetUserName | pgustavo
```



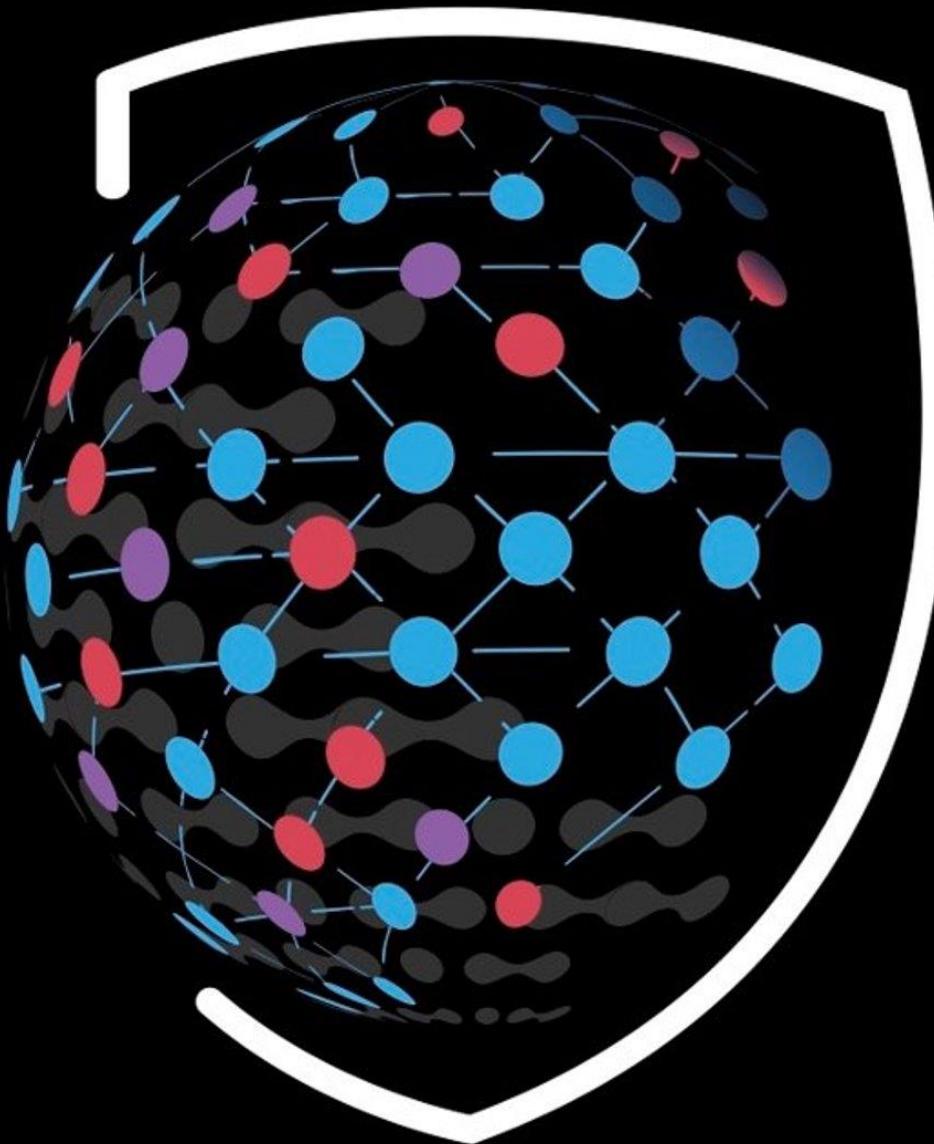
Que planes para el futuro de Mordor?

Desde casa!



2020 - End of the Year

- Cobertura de plataformas (Colección de data)
 - Azure
 - Linux(Ubuntu 16 & 18)
- Mordor Data Injection
 - Una forma de transformar un set de datos para que paresca que fue creado en un ambiente específico
- Mas Datasets siguiendo planes de emulación creados por la comunidad:
 - https://github.com/center-for-threat-informed-defense/adversary_emulation_library



OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY

Sigamos Conversando y Unete al OTR Discord

- Roberto Rodriguez **@Cyb3rWard0g**
- Jose Rodriguez **@Cyb3rPandaH**
- OTR Discord Link (Invitación automática)
 - **bitly.com/OTRDiscord**
 - Acepta el CAPTCHA
 - Lee y acepta el código de conducta de nuestro discord



Muchas Gracias!