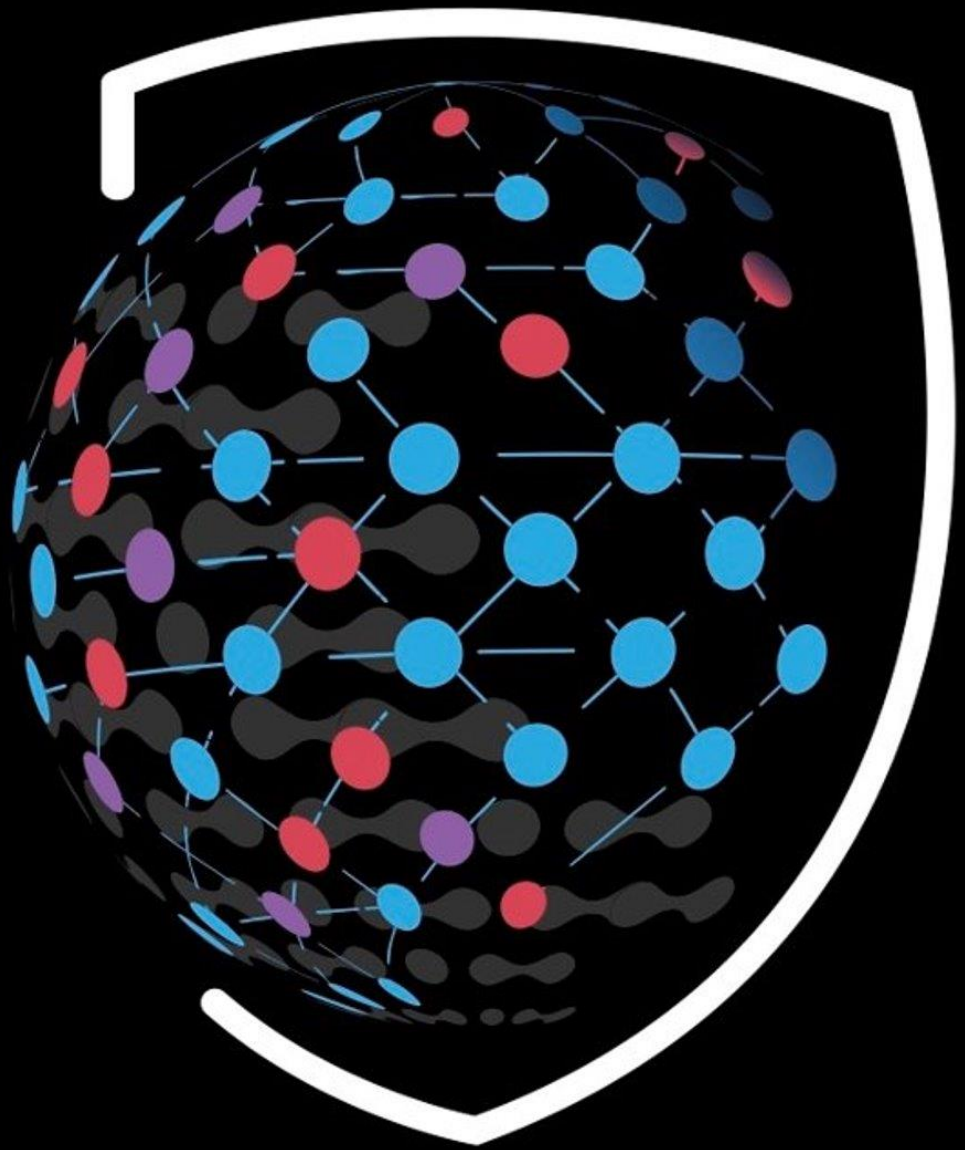


OPEN THREAT RESEARCH

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 Codigo Abierto ♡ @OTR_Community
- Threat Hunter Playbook @HunterPlaybook
- Mordor @Mordor_Project
- OSSEM @OSSEM_Project
- Blacksmith & more..

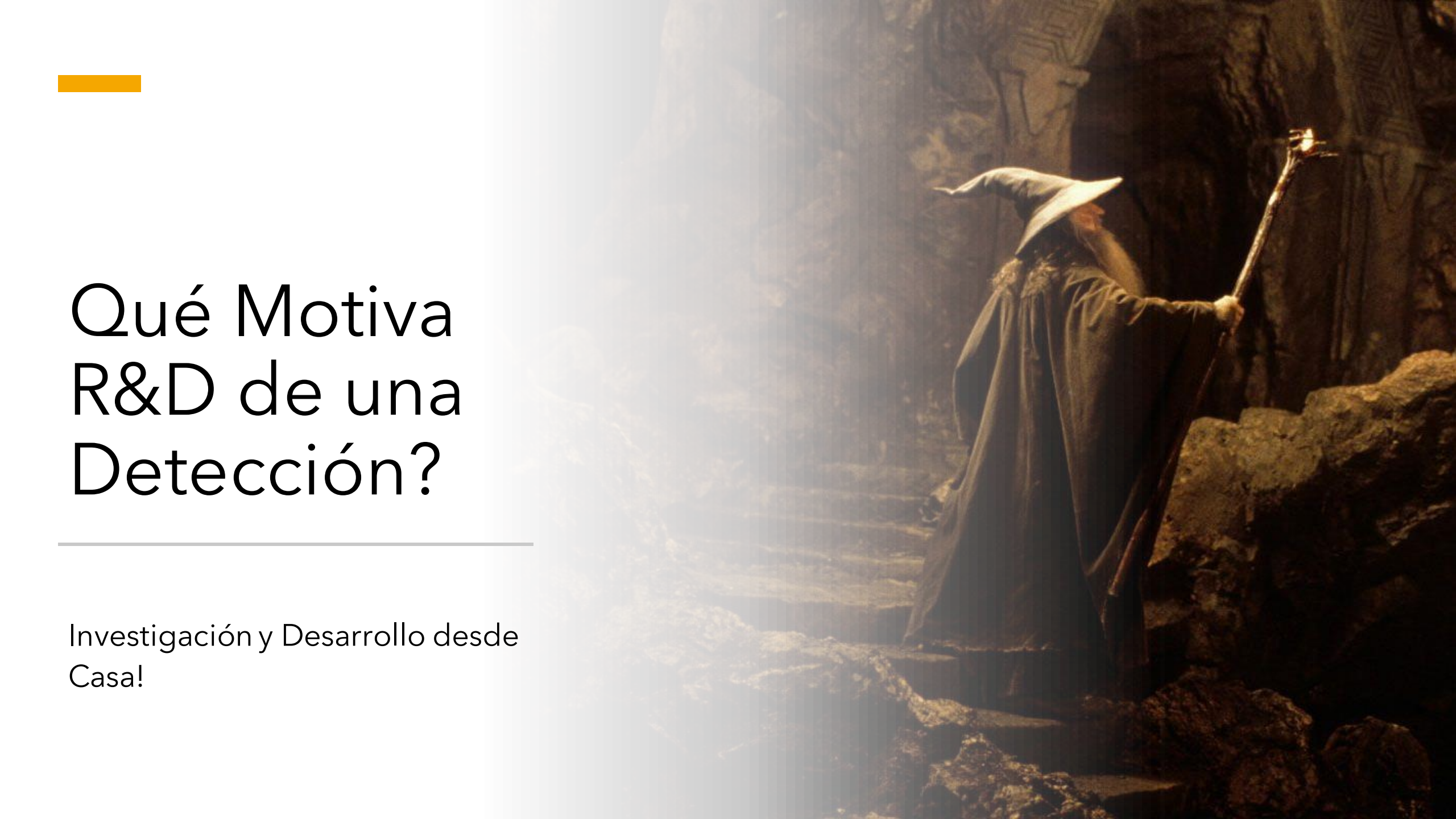
https://github.com/OTRF

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?

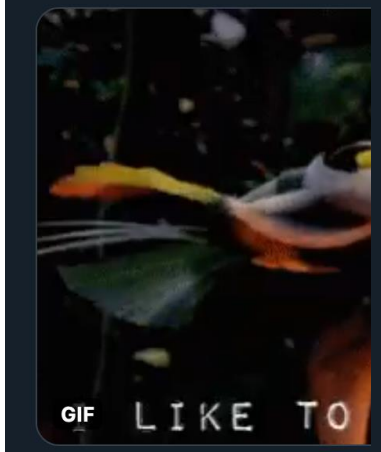
Investigación y Desarrollo desde Casa!



Hoy en día...

MDSec
@MDSecLabs

Part 1 in the "I Like to Mo
@domchell is now live... r



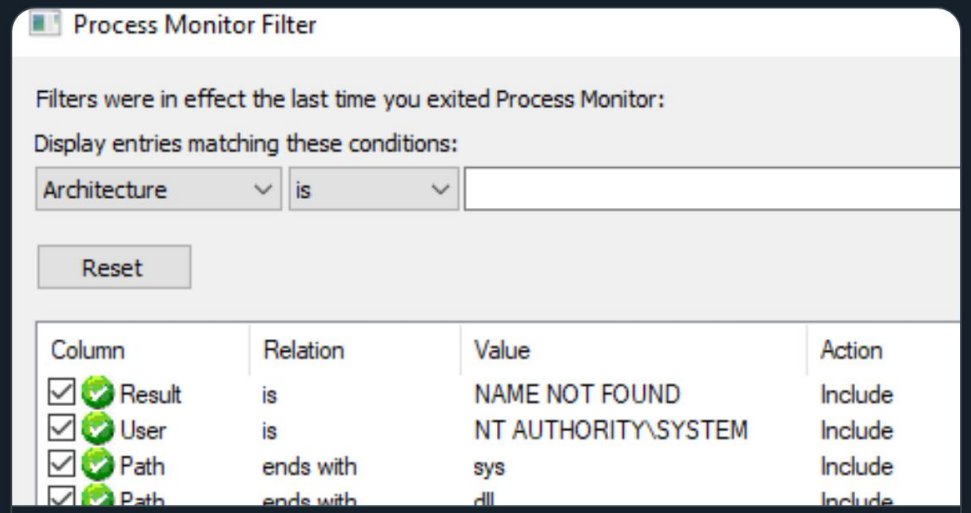
9:26 AM · Sep 1, 2020 · Twitter

120 Retweets **4** Quote Twee

6

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!



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

1 103 183

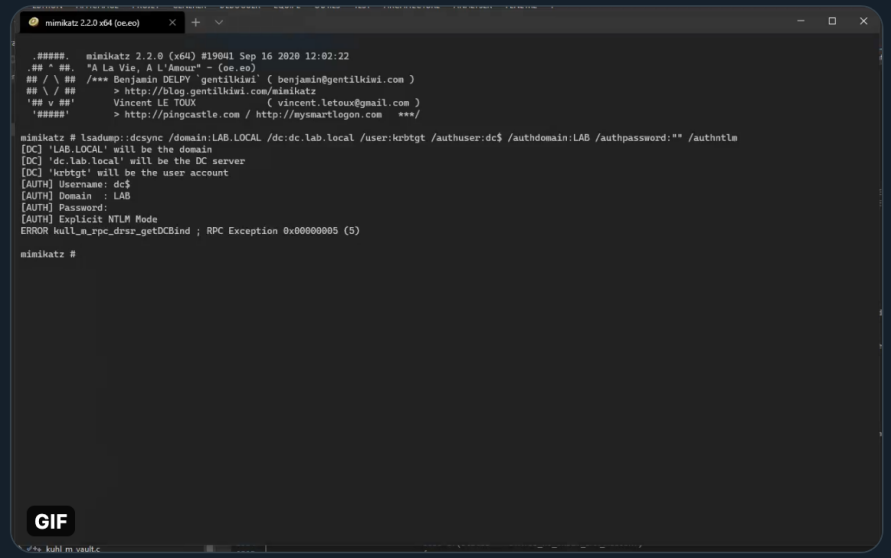
Benjamin Delpy
@gentilkiwi

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...

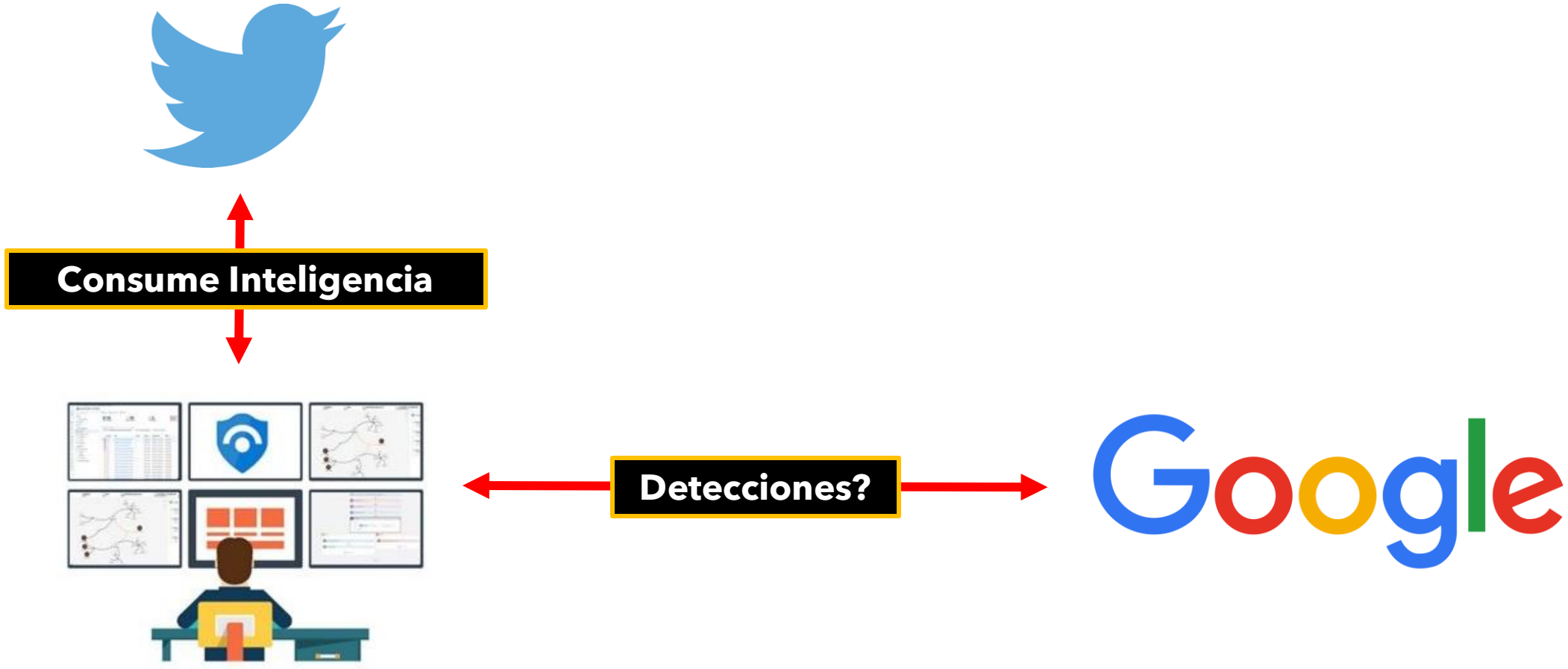
Thank you: @SecuraBV



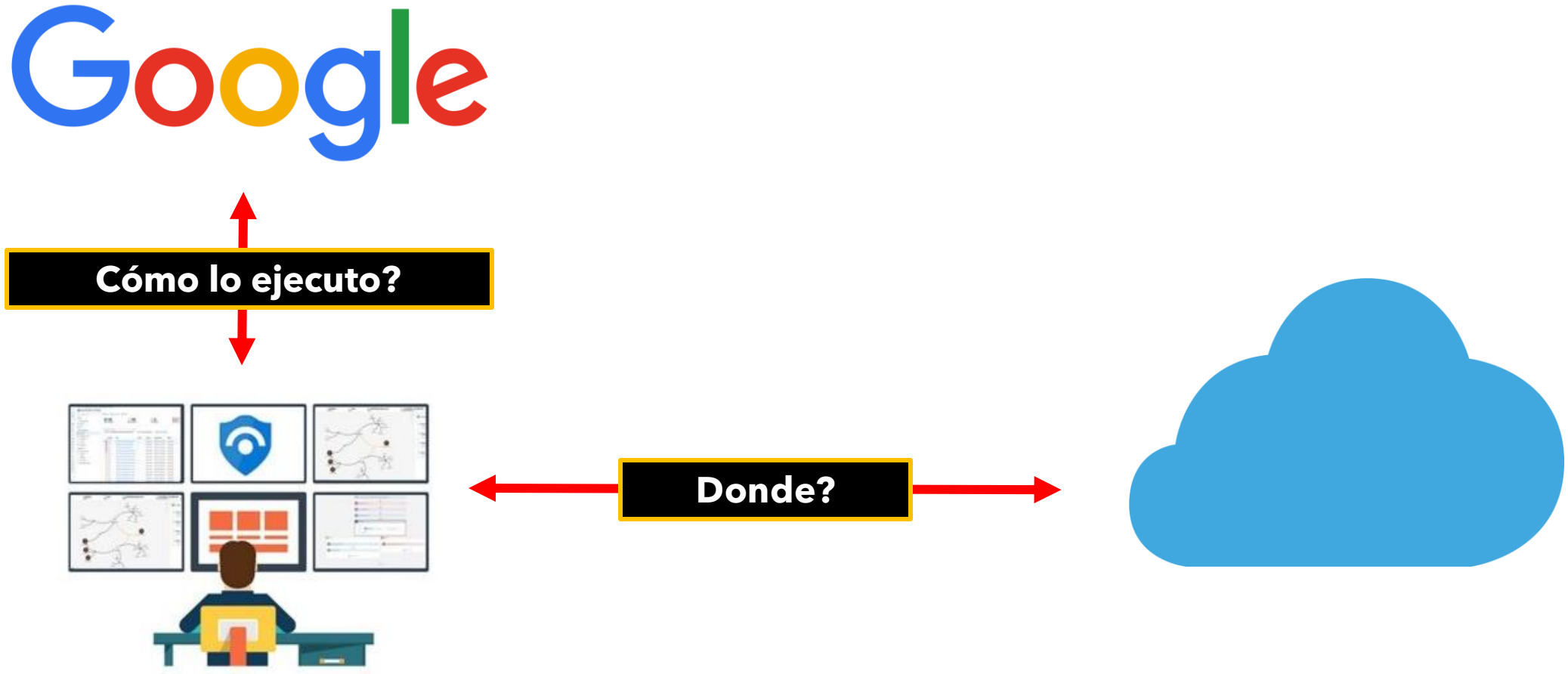
6:30 AM · Sep 16, 2020 · Twitter Web App

643 Retweets **34** Quote Tweets **1K** Likes

Qué hago? Alguien en la comunidad?



Lo Simulas de Una? Qué Necesitas?

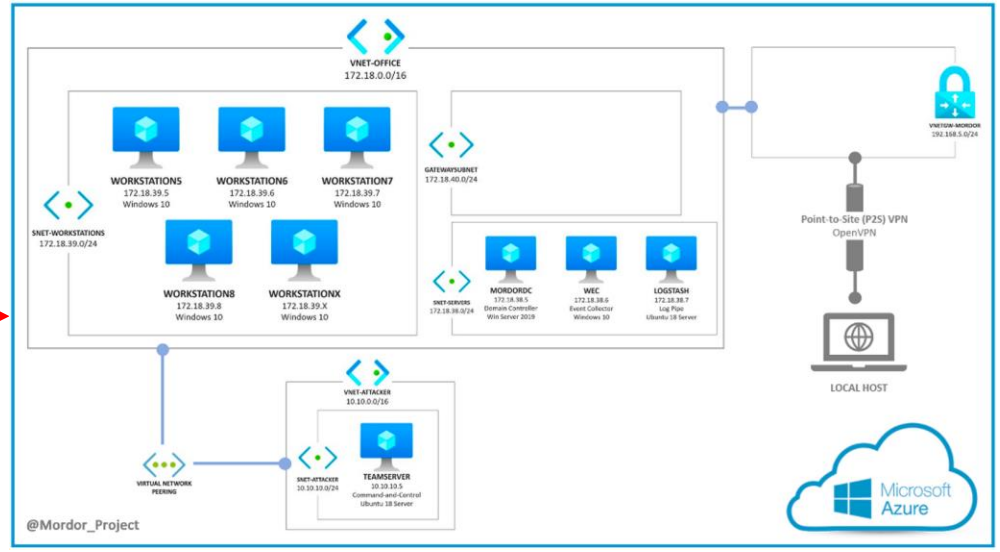


Requiero de una o más computadoras?

Google

Como lo ejecuto?

Dónde?



Una Metodología Básica!

La que usamos! 😉


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)


Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)


Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos


Resumir
Filtrar
Correlacionar
Visualizar


Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Resumir
Filtrar
Correlacionar
Visualizar


Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)


Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos


SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)

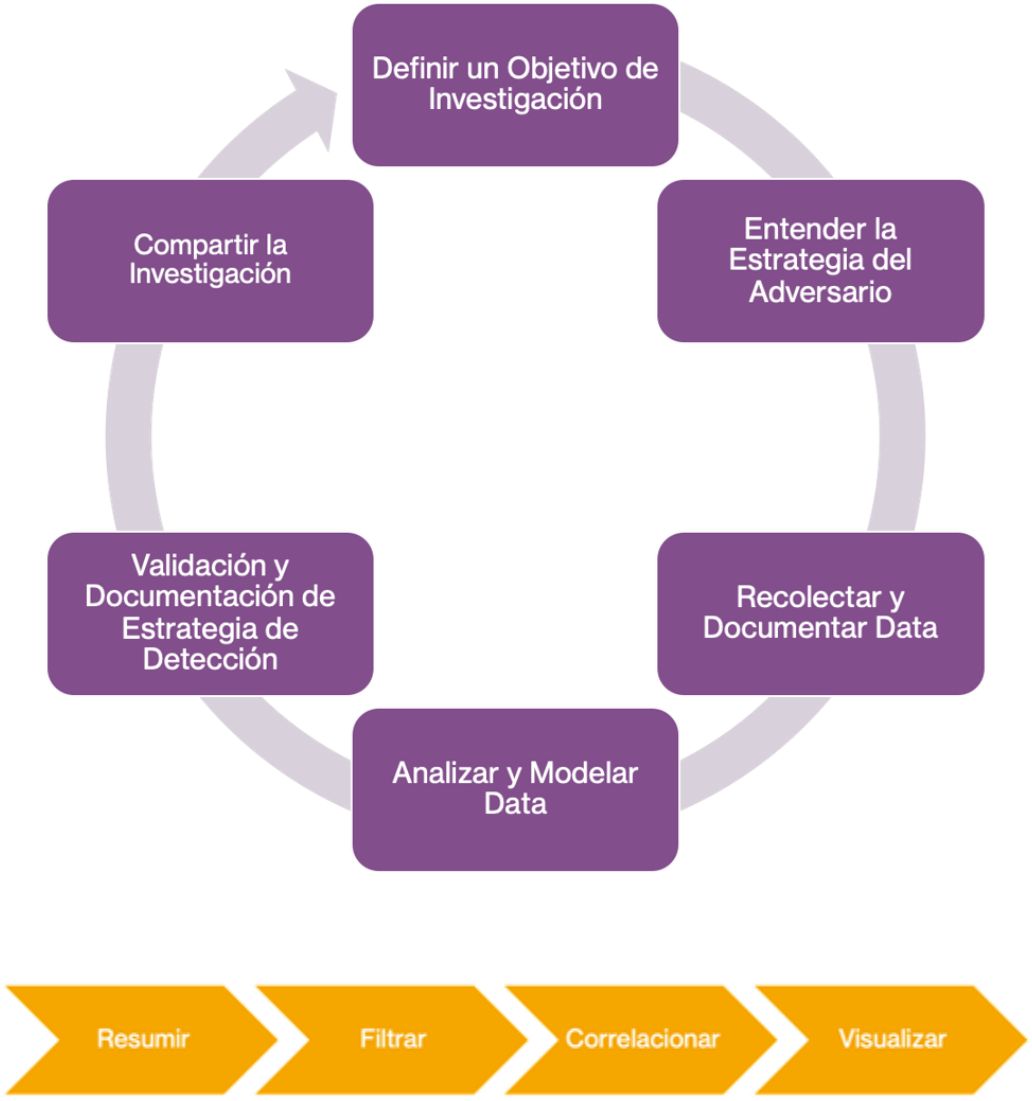

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Resumir
Filtrar
Correlacionar
Visualizar


Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos


SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad


Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación
Resumir
Filtrar
Correlacionar
Visualizar


Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)


Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos

Simulando al Adversario!

Desde casa!

Actividades Básicas al simular al adversario

Planificación

Emulacion

Habilitar telemetría

Recolectar y analizar datos

Puedo detectarlo?

No

Si

Documentar Resultados

Más que validar controles de seguridad!!

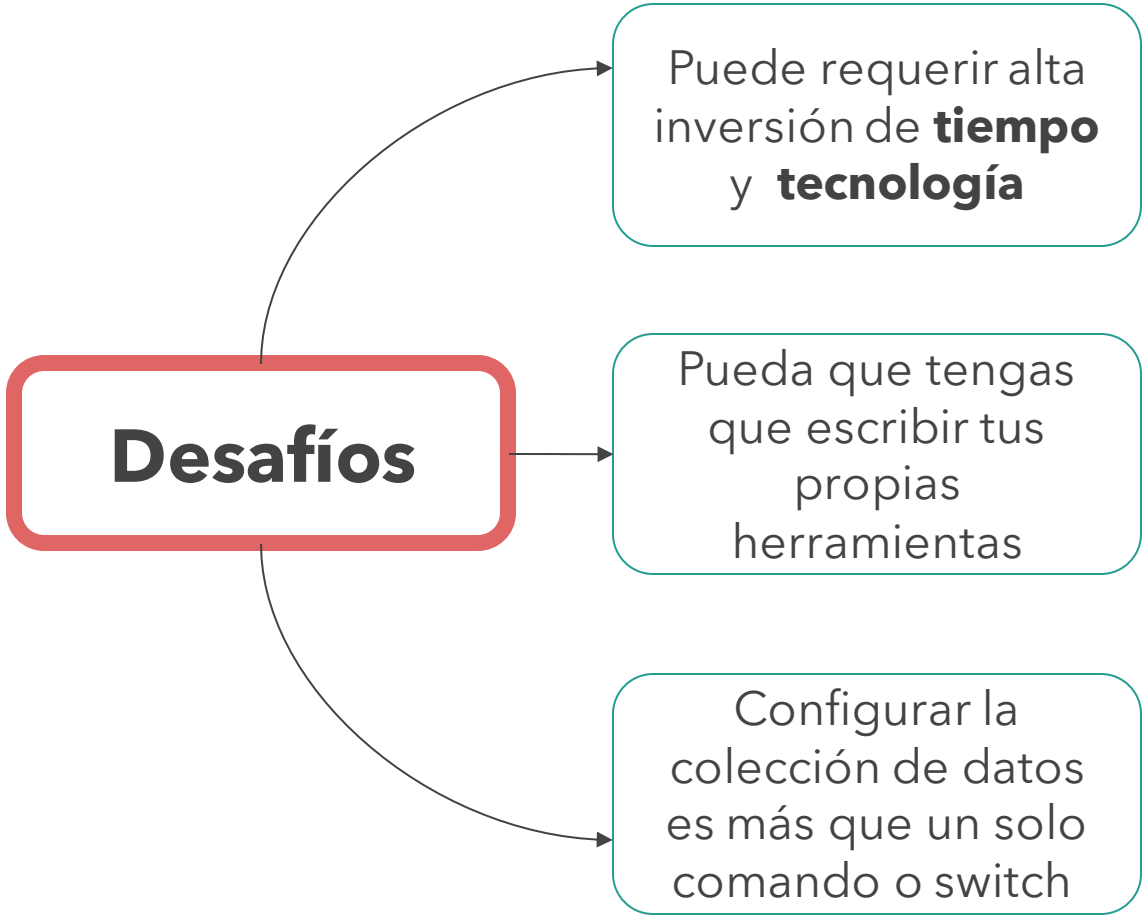
Beneficios

- Documentación y modelamiento de nuevas técnicas
- Mejorar y complementar detecciones
- **Identificación de oportunidades para mejorar la colección de datos**

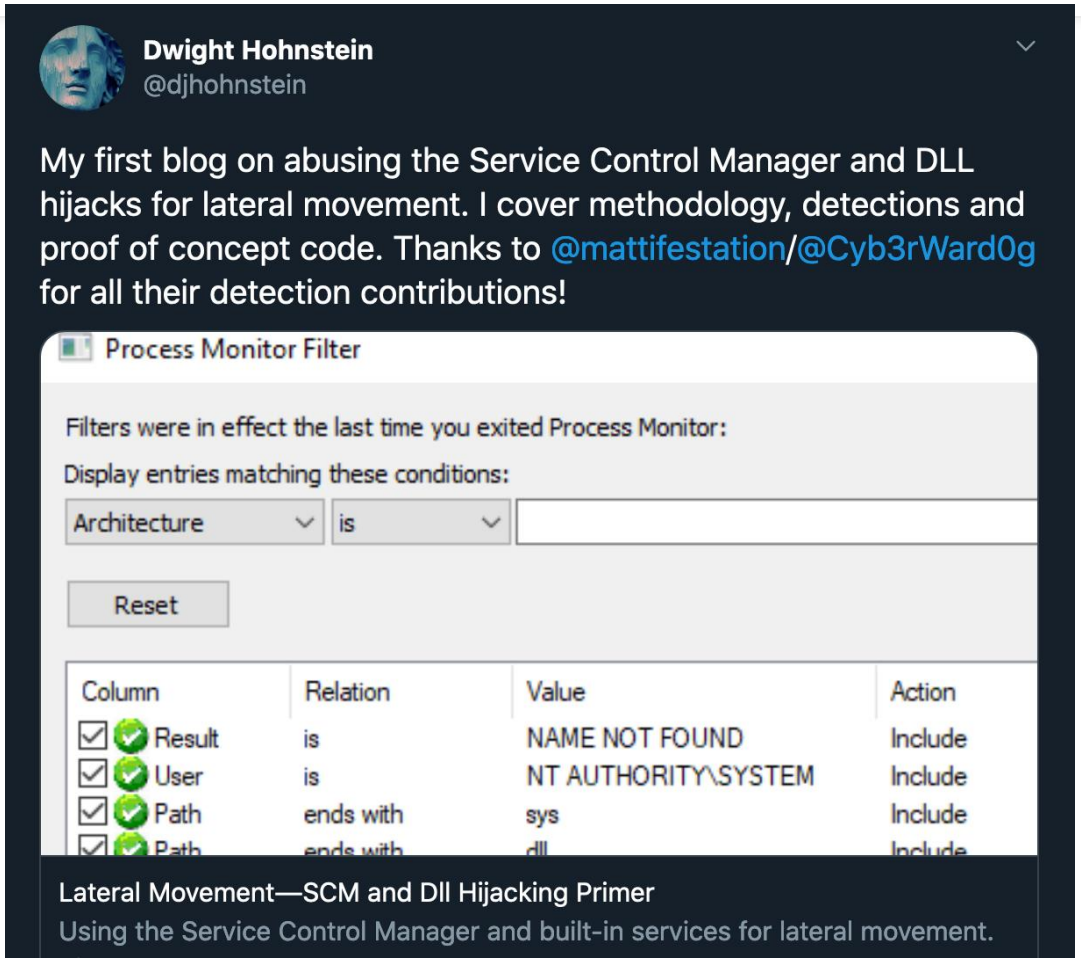
Cómo? Dónde? Cuándo? Whát 🤔? (Spanglish)

Planificación	Emulación
	
Recolectar y Analizar	**Habilitar Telemetría**
	

Documentar resultados

No nos crees 😂? Un ejemplo básico..



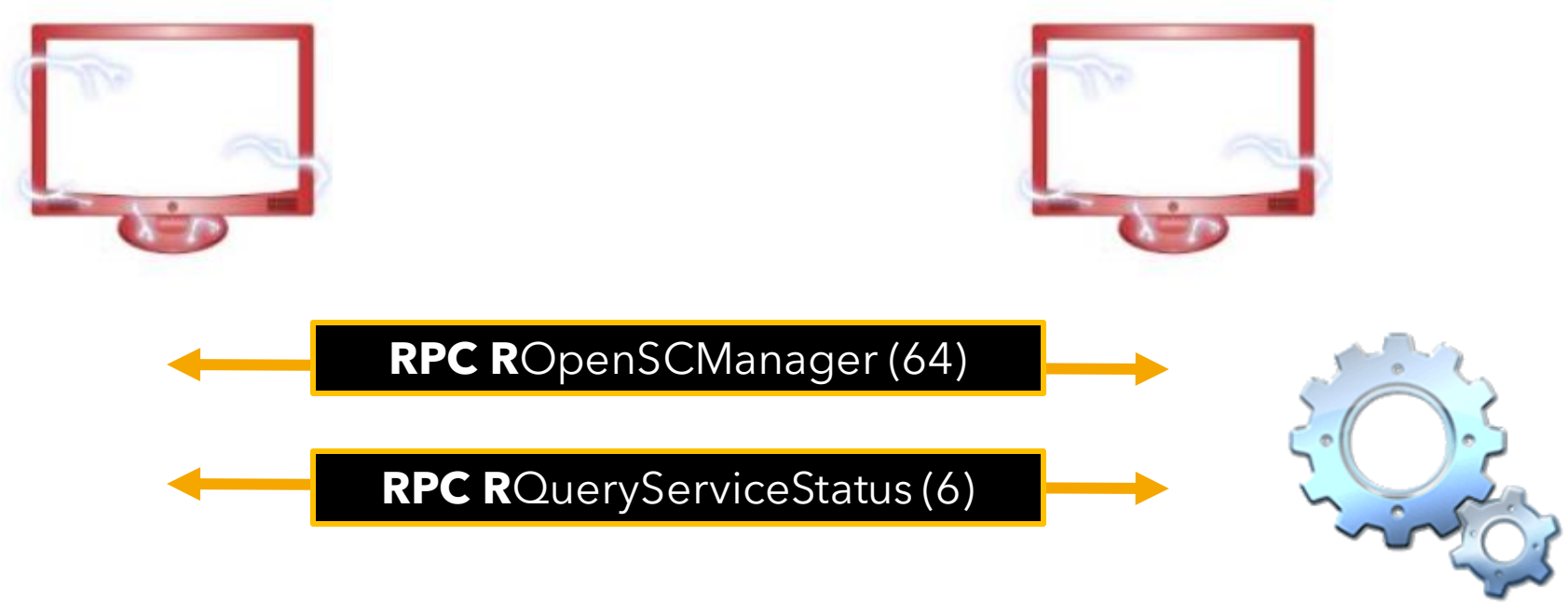
https://twitter.com/djhohnstein/status/1118865501466308608

Abusando de el SCM y DLL Hijacks!

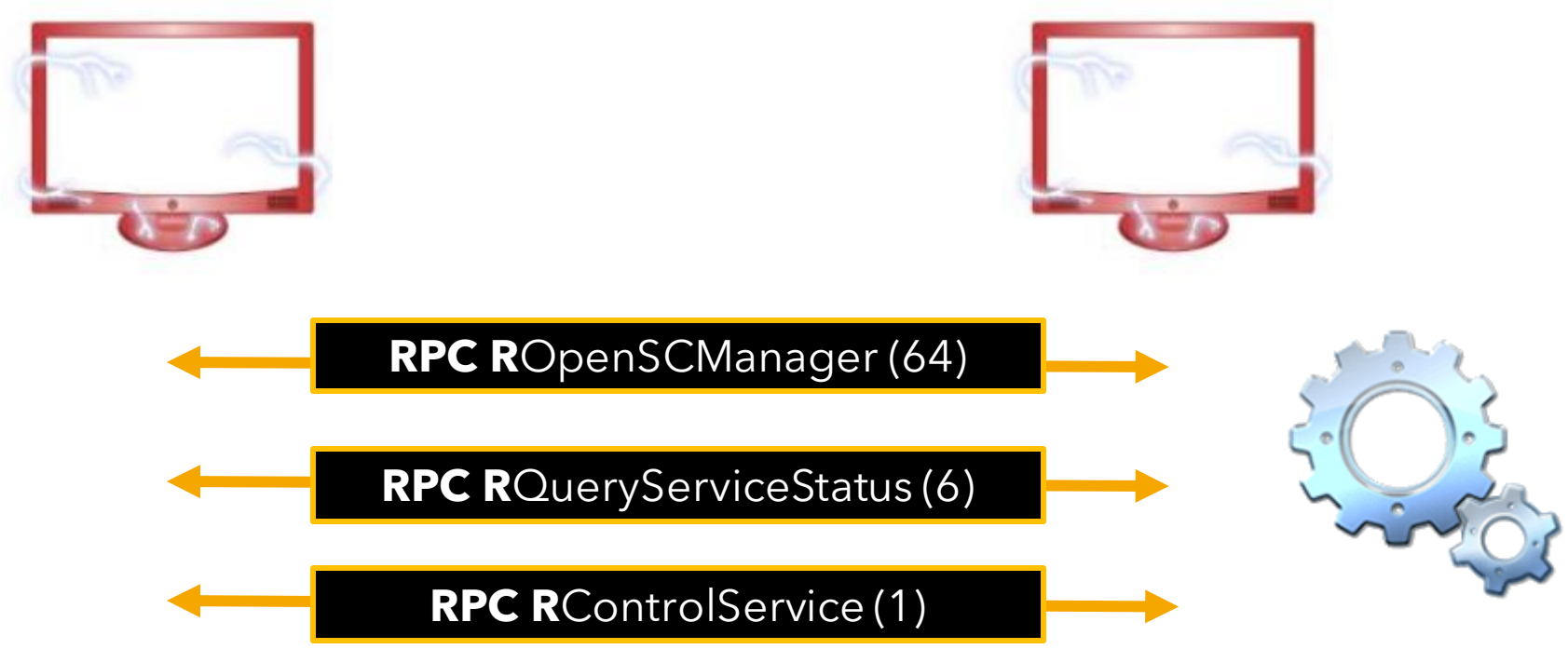
Abusando de el SCM y DLL Hijacks!

Servicio Vulnerable Identificado

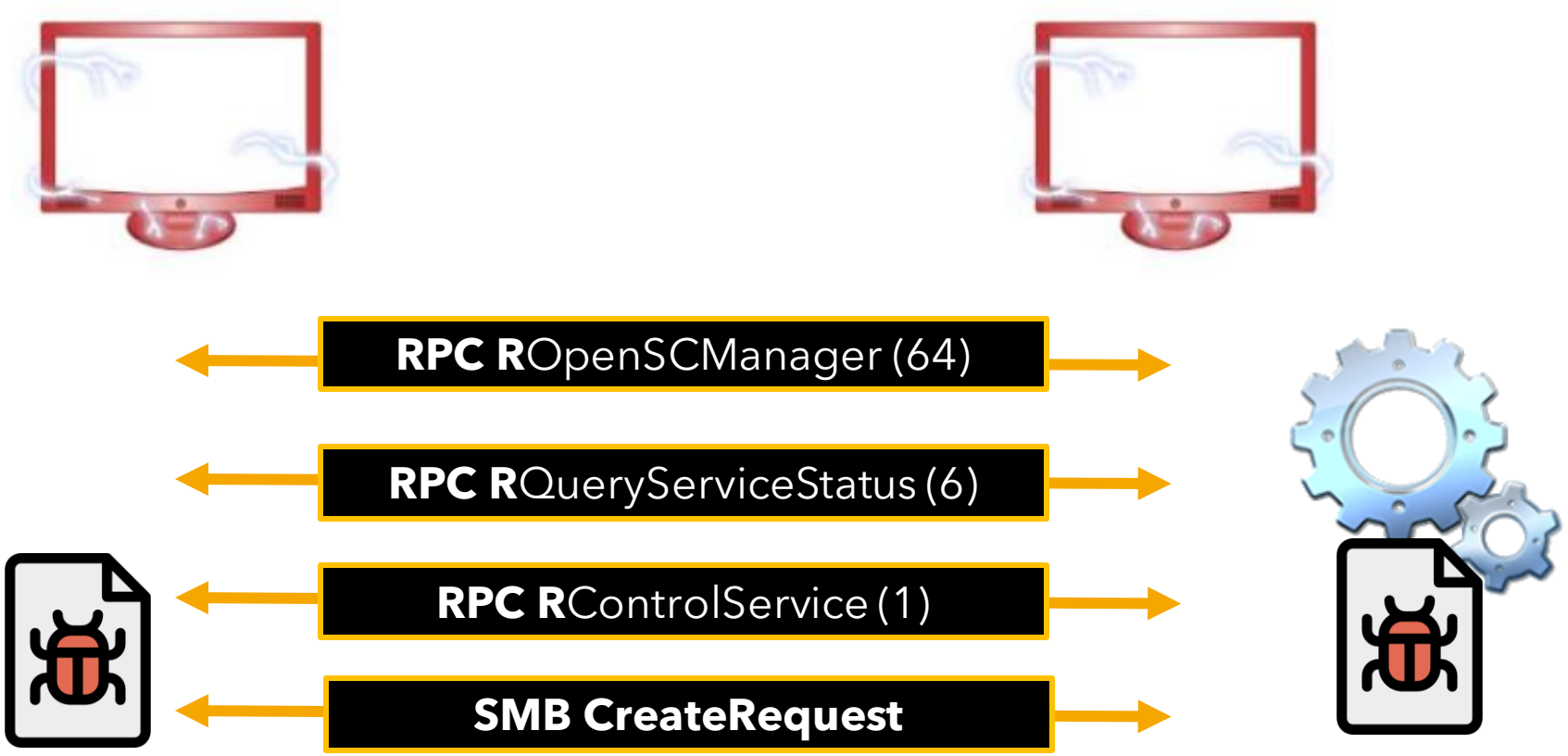
Abusando de el SCM y DLL Hijacks!



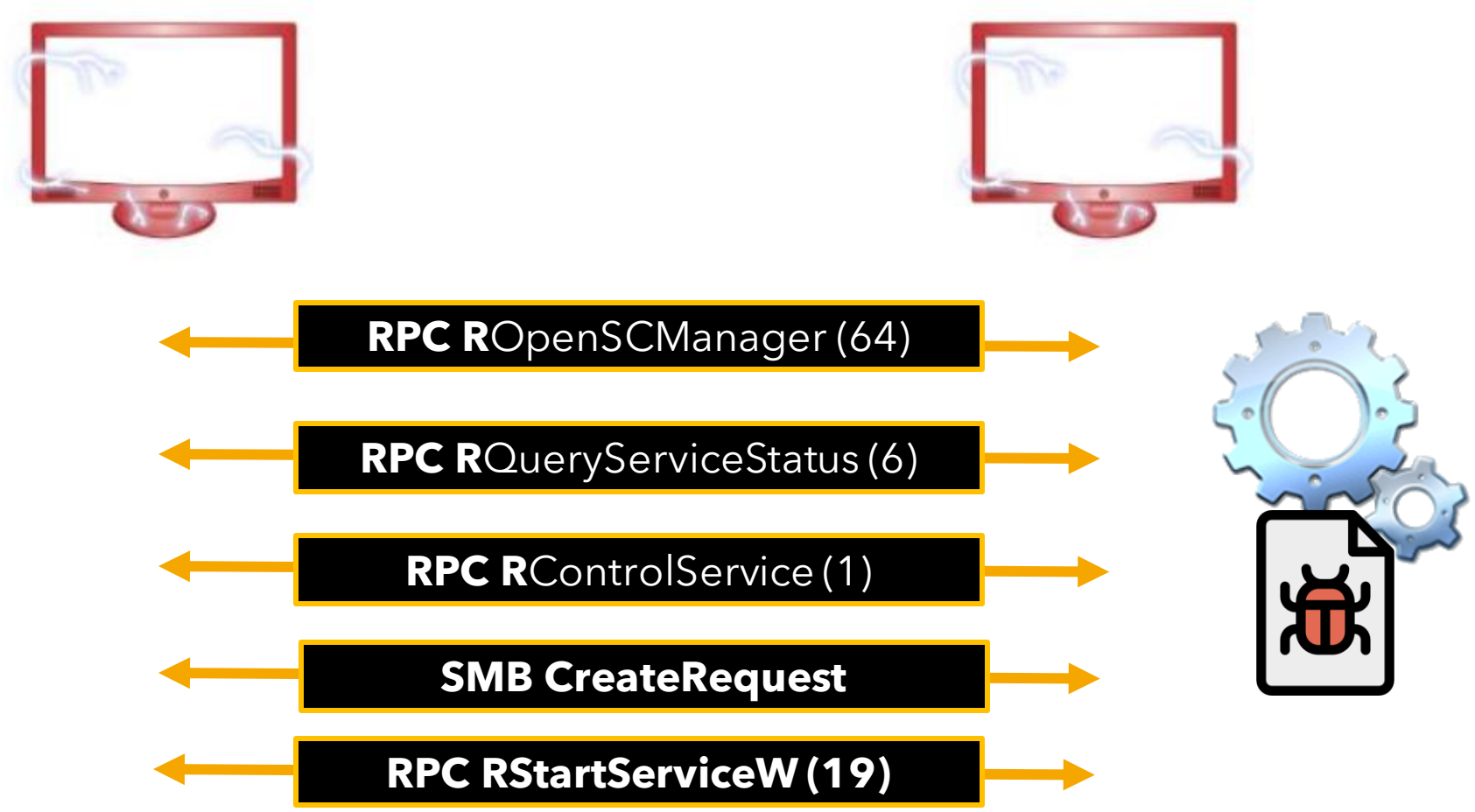
Abusando de el SCM y DLL Hijacks!



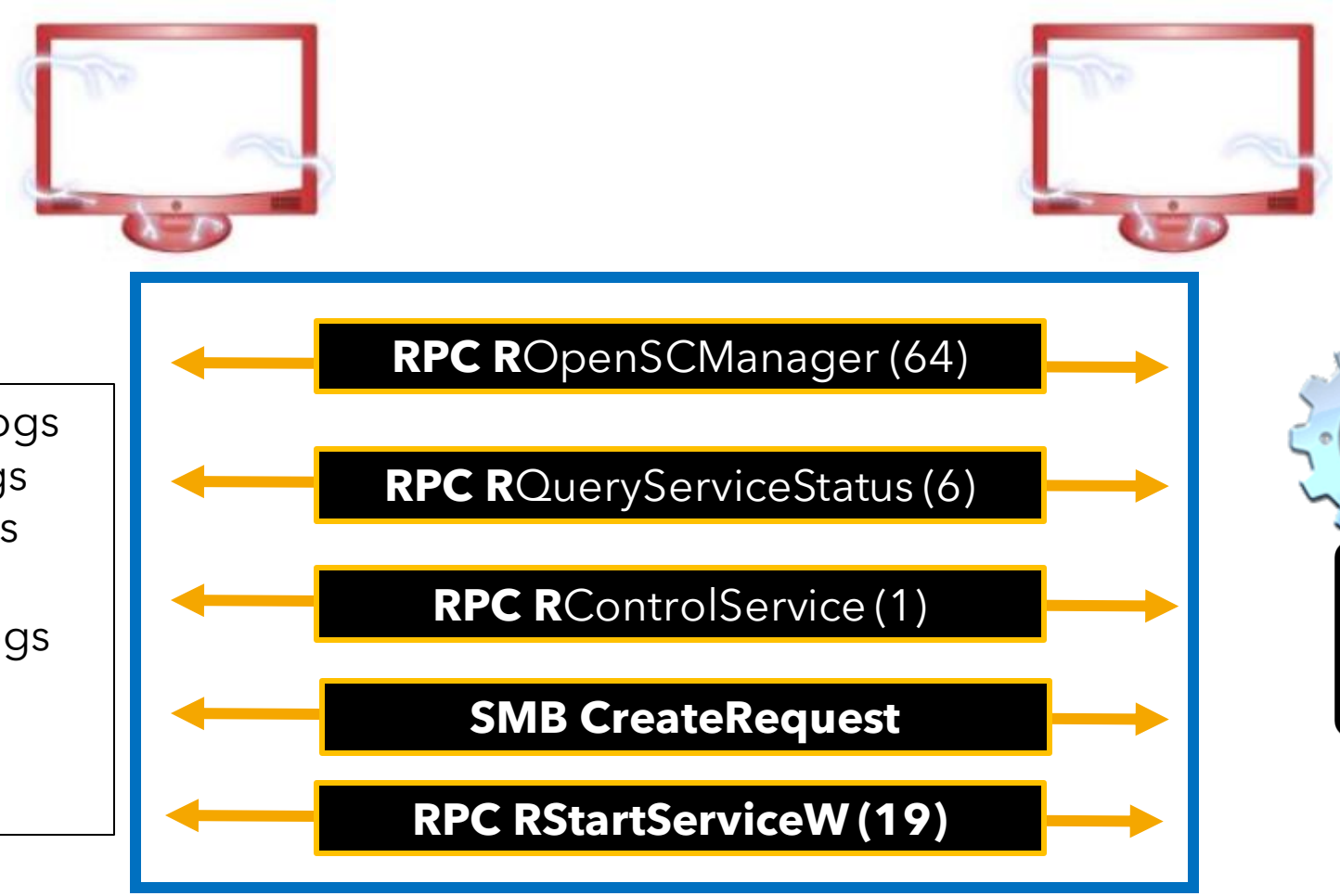
Abusando de el SCM y DLL Hijacks!



Abusando de el SCM y DLL Hijacks!



Qué necesito?: Pólizas de Auditoria



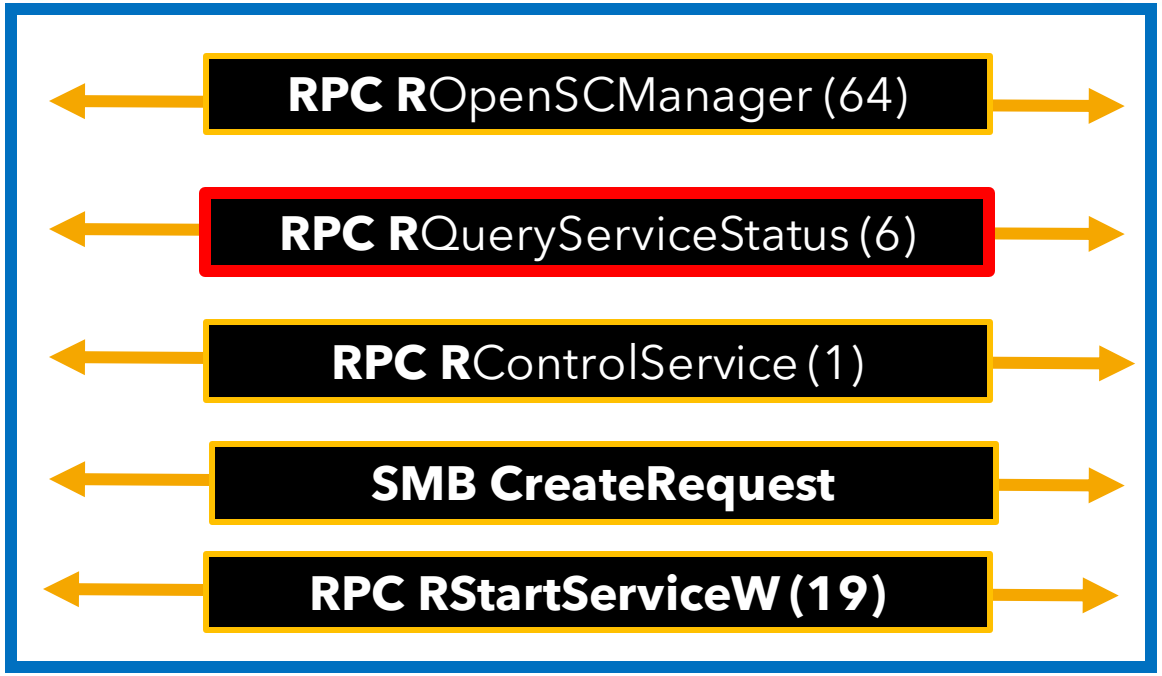
- Regla de auditoria para el servicio vulnerable?
- Regla de auditoria para el SCM?

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

Cómo respondo a las variaciones?

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

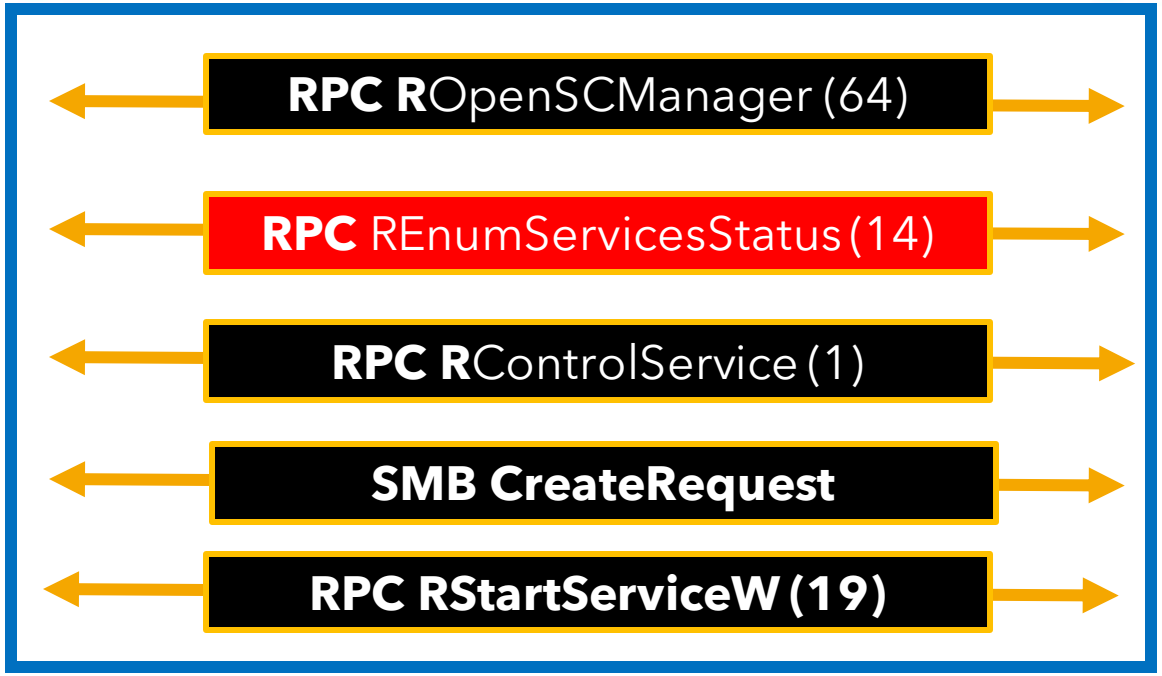
- Authentication Logs
- Share Access Logs
- File Creation Logs
- SCM Logs?
- Object Access Logs
- Packet Capture
- System Logs?



Qué pasa si el servicio no es tocado?

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

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

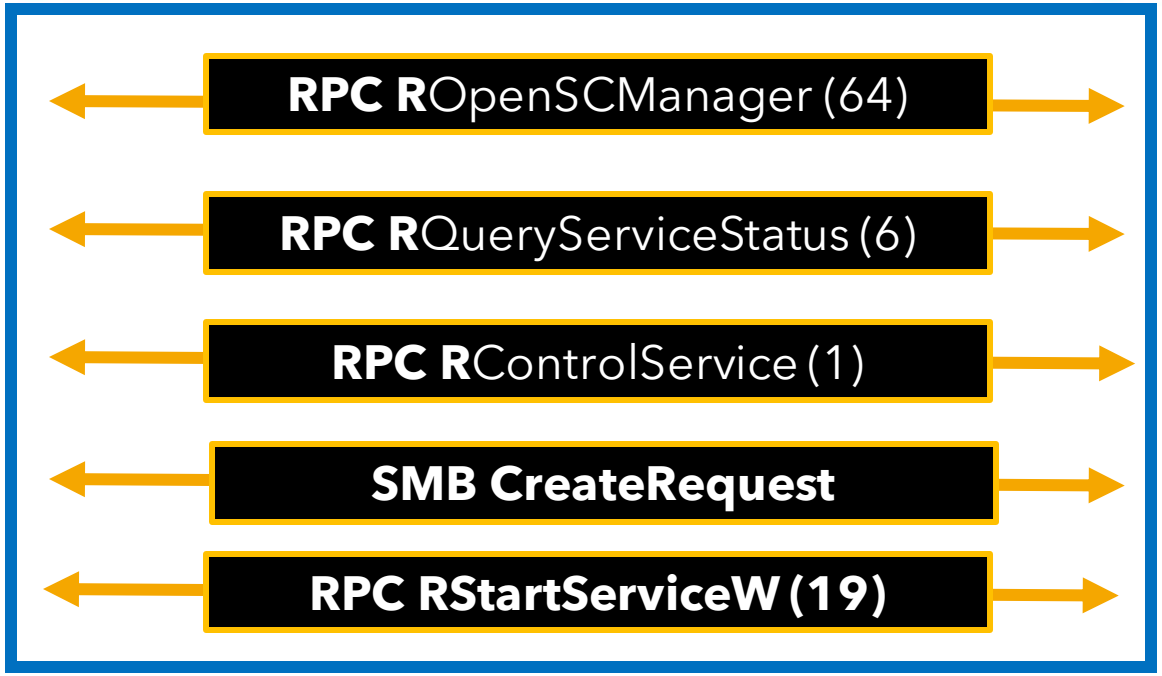


Qué herramientas? Qué infraestructura?

- Infraestructura
- Herramientas (SC.exe? Codigo Libre? C2?)

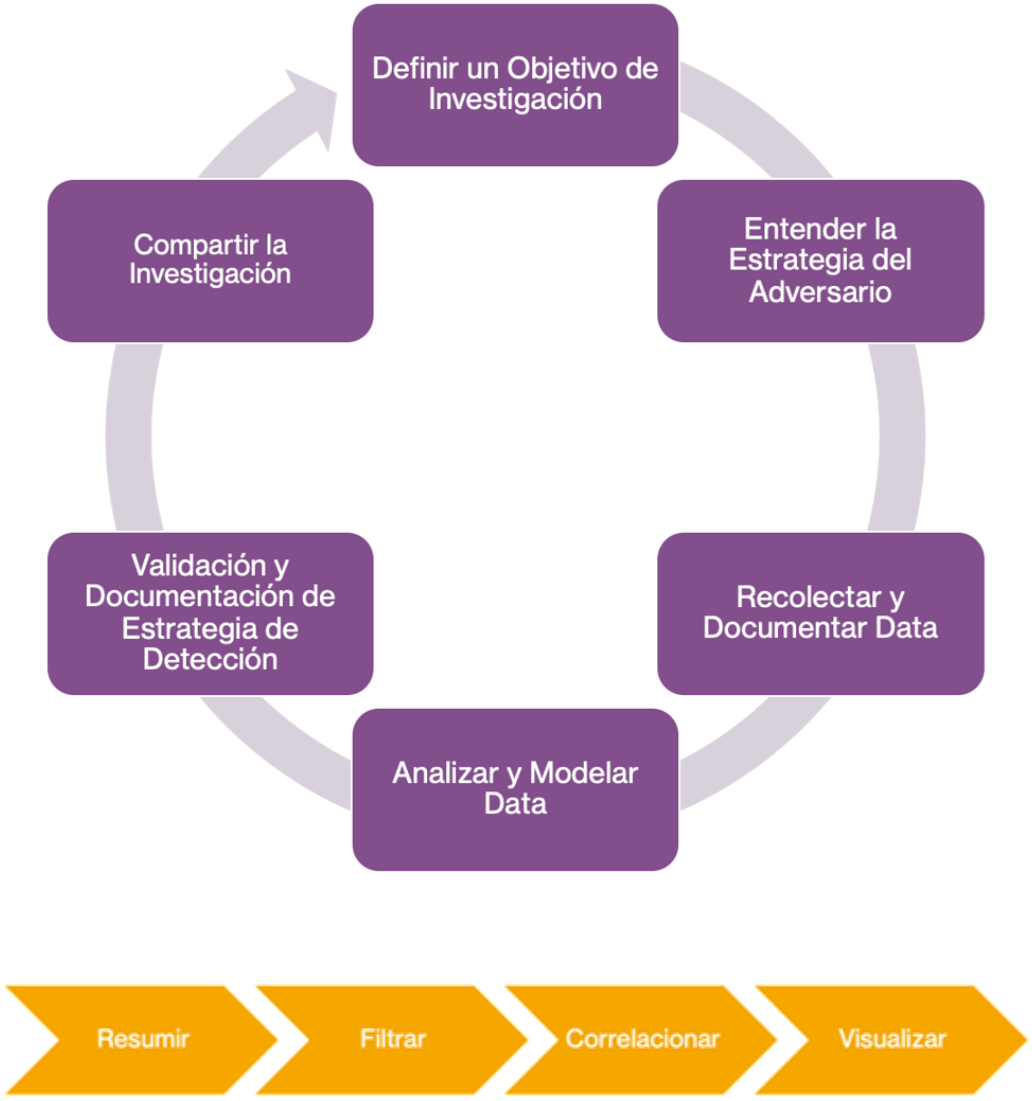
- Regla de auditoria para el servicio vulnerable?
- Regla de auditoria para el SCM?

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




SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad

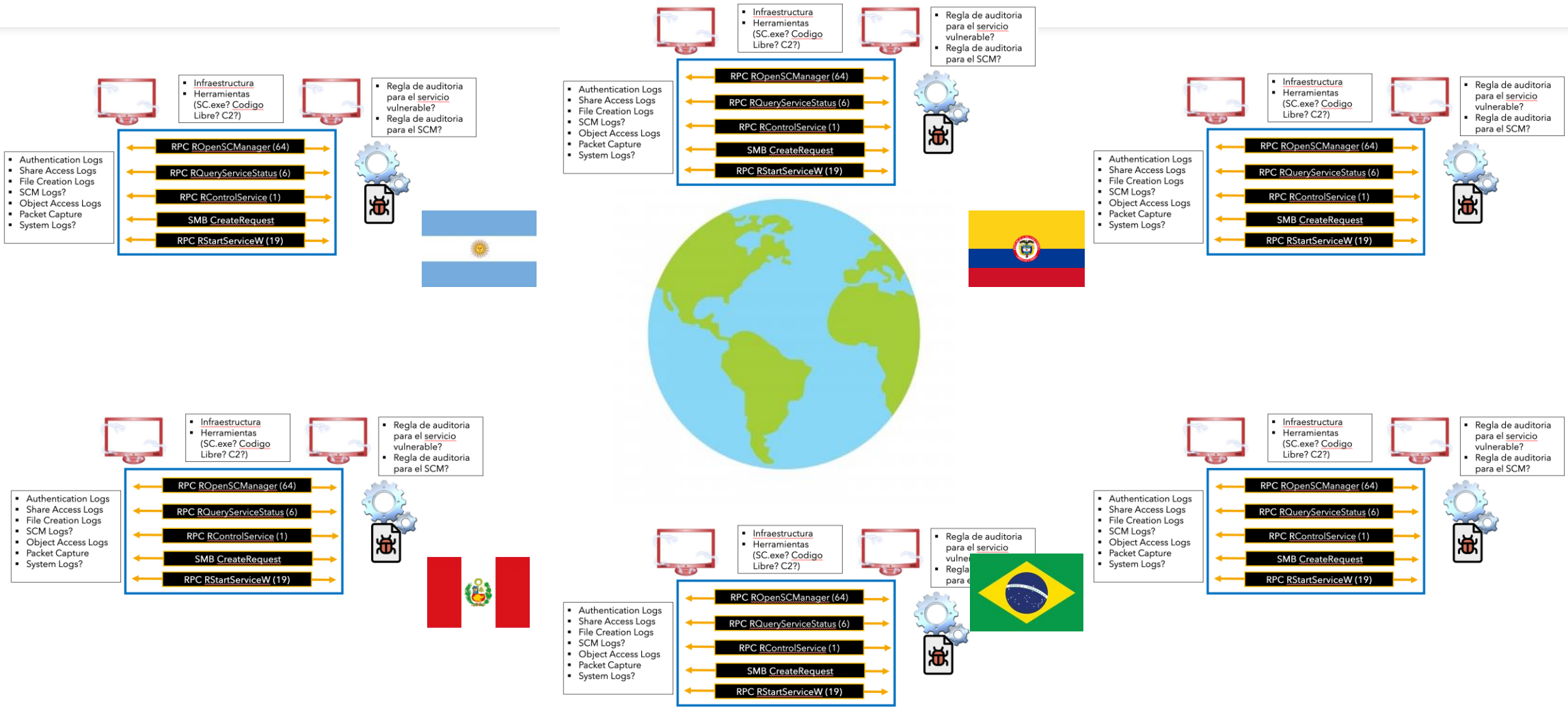

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación
Resumir
Filtrar
Correlacionar
Visualizar

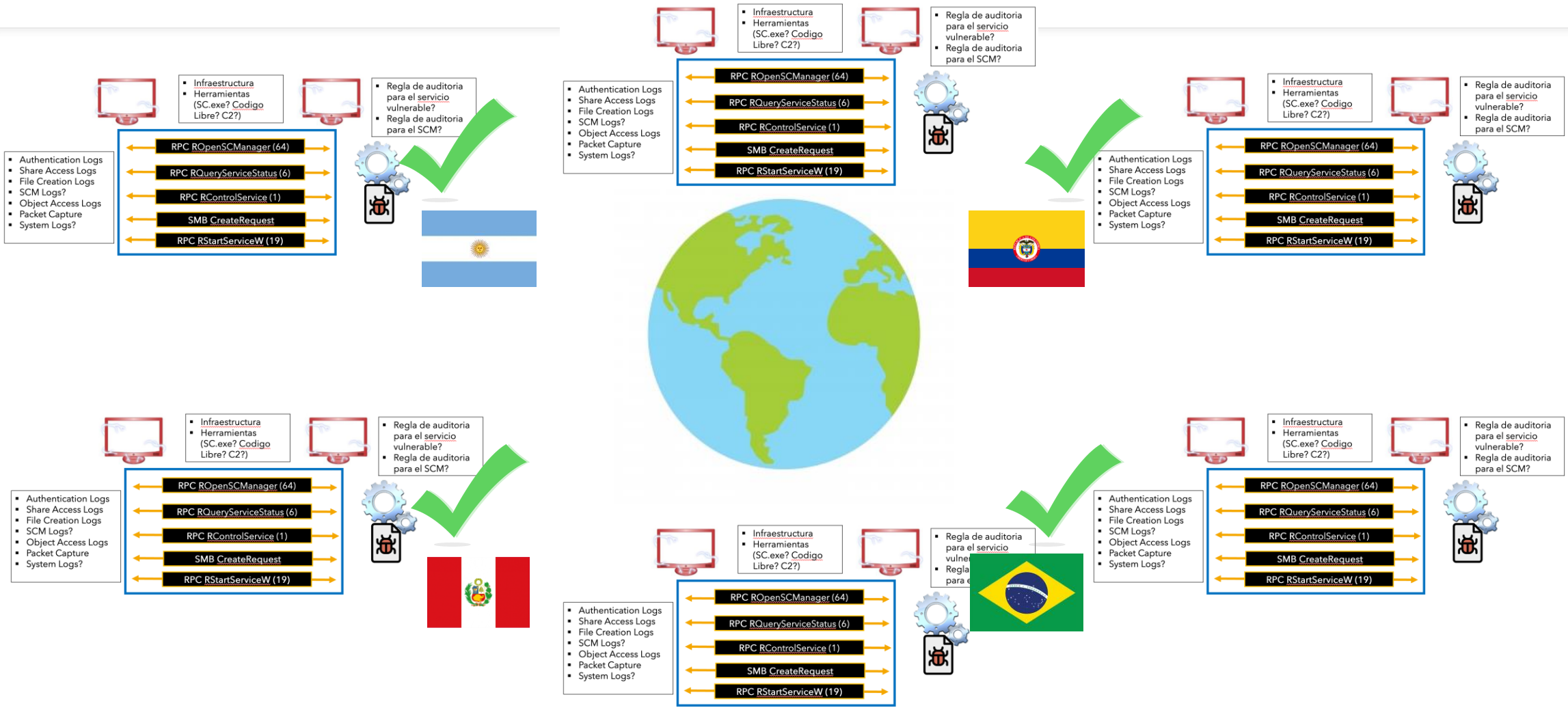

Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)


Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos

En todas partes de el mundo...



En todas partes de el mundo..



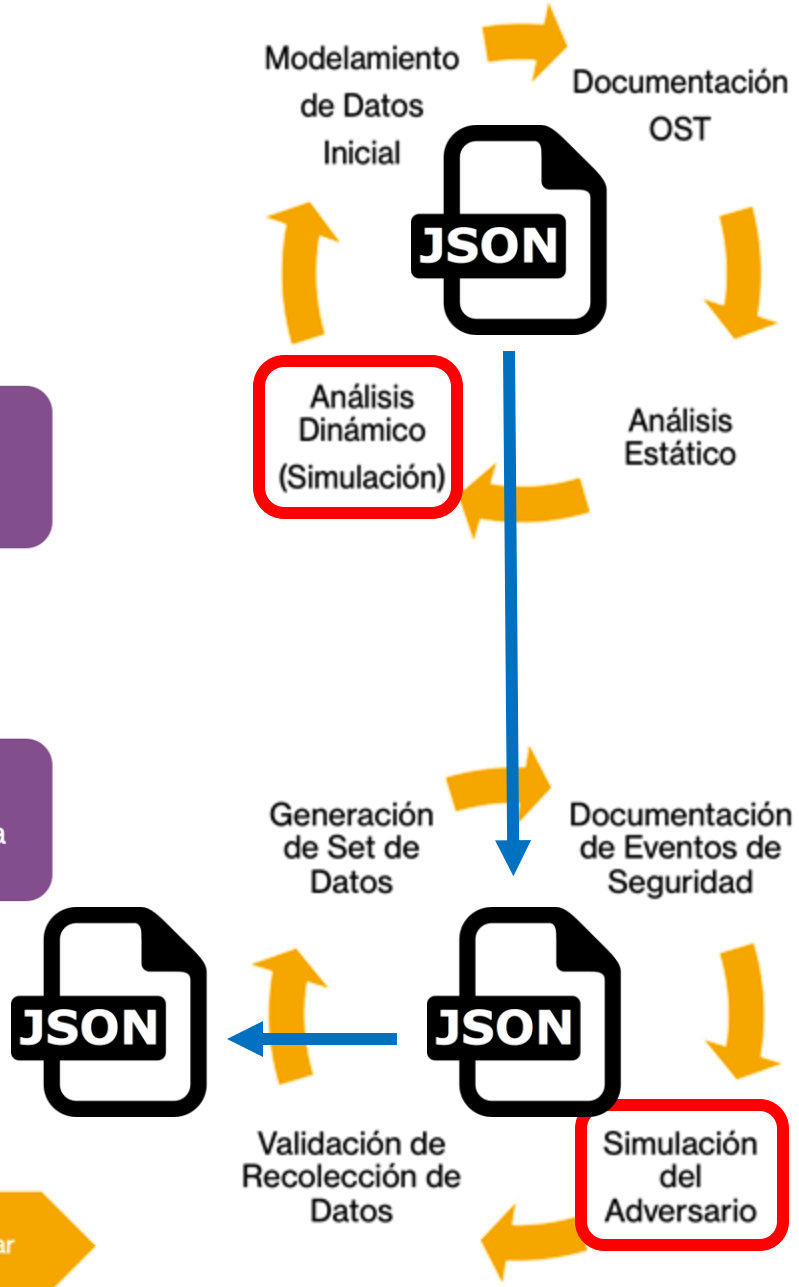
En todas partes de el mundo..


SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad


Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


Resumir
Filtrar
Correlacionar
Visualizar


Modelamiento de Datos Inicial
Documentación OST
JSON
Análisis Dinámico (Simulación)
Análisis Estático
Generación de Set de Datos
Documentación de Eventos de Seguridad
JSON
JSON
Validación de Recolección de Datos
Simulación del Adversario

Bienvenidos a Mordor

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

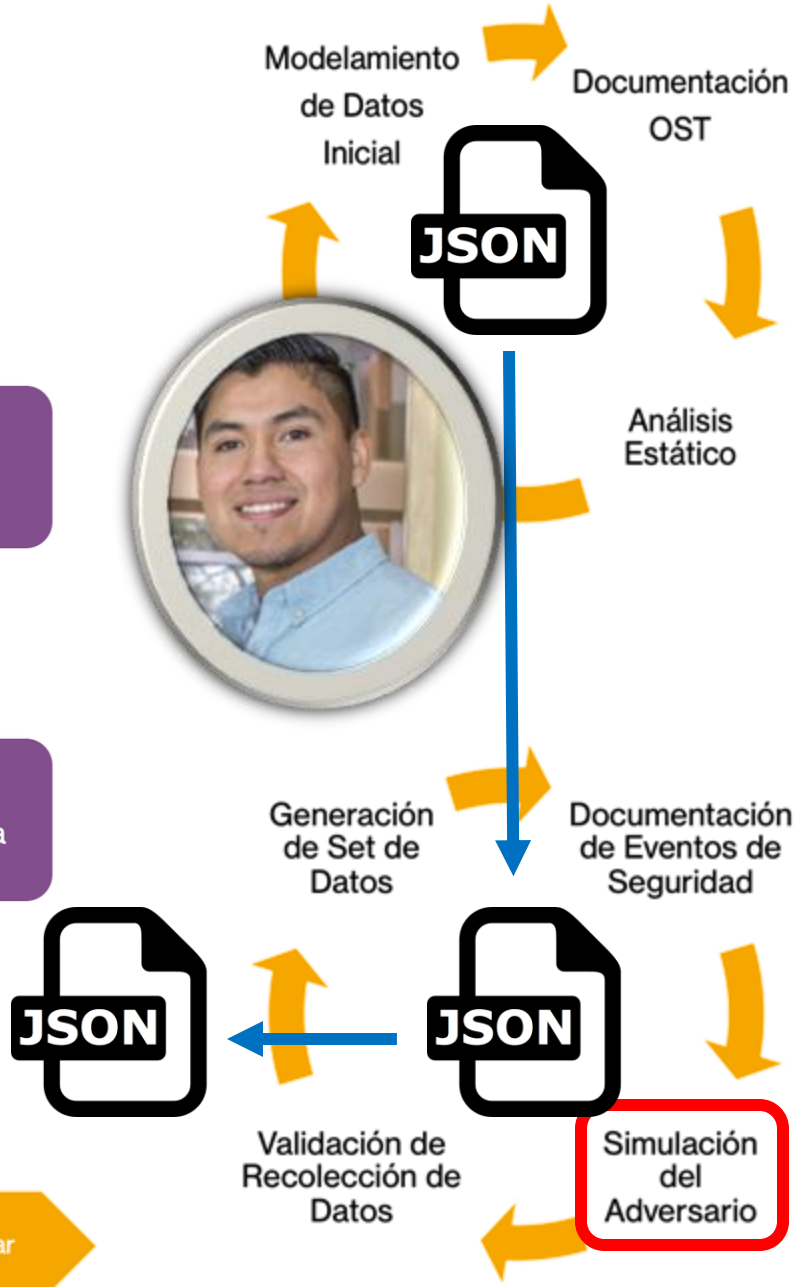
@Mordor_Project

- 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

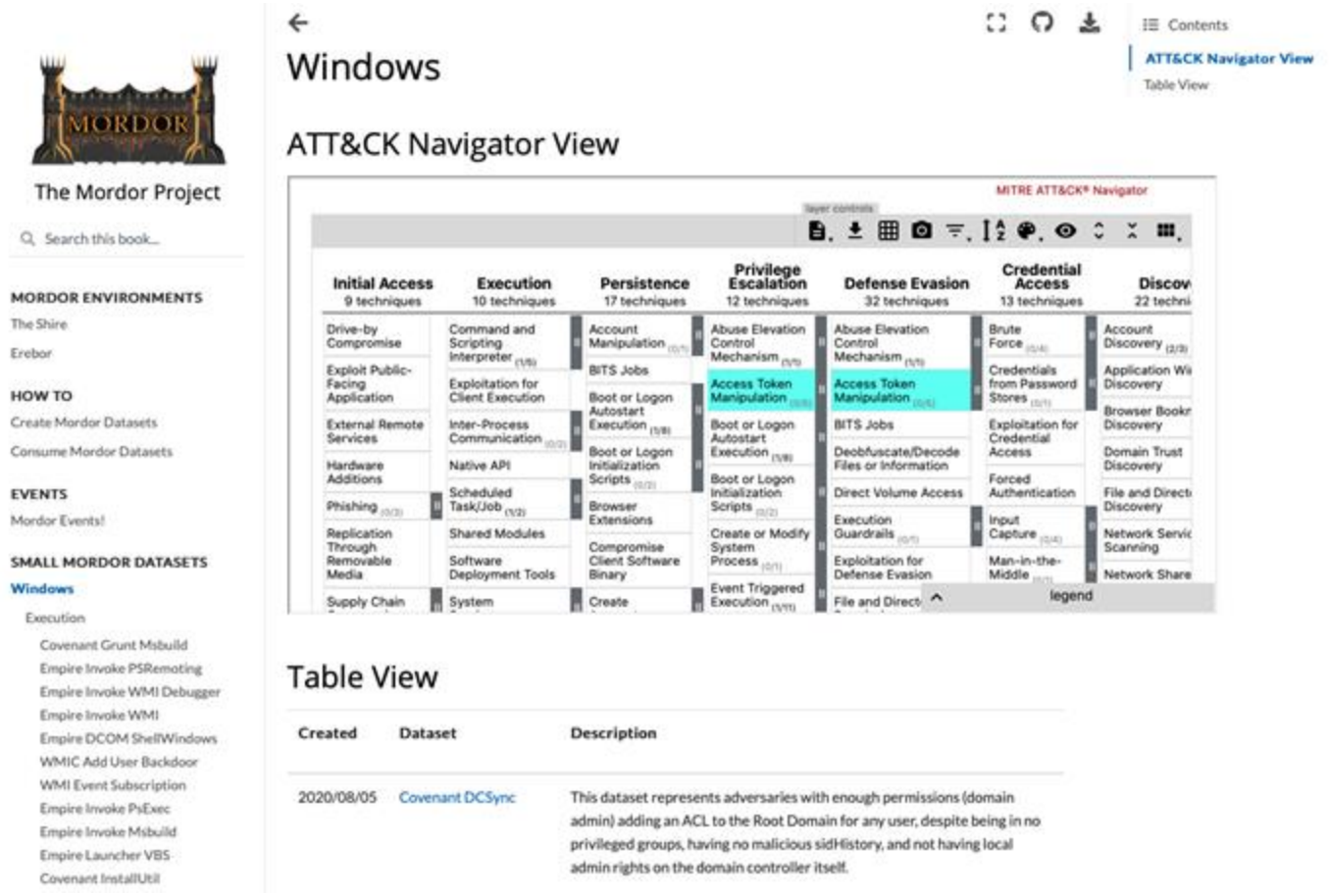

SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad


Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación
Resumir
Filtrar
Correlacionar
Visualizar


Modelamiento de Datos Inicial
Documentación OST
JSON
Análisis Estático
Generación de Set de Datos
Documentación de Eventos de Seguridad
JSON
JSON
Validación de Recolección de Datos
Simulación del Adversario

https://mordordatasets.com



Tecnicas especificas
(Small datasets)

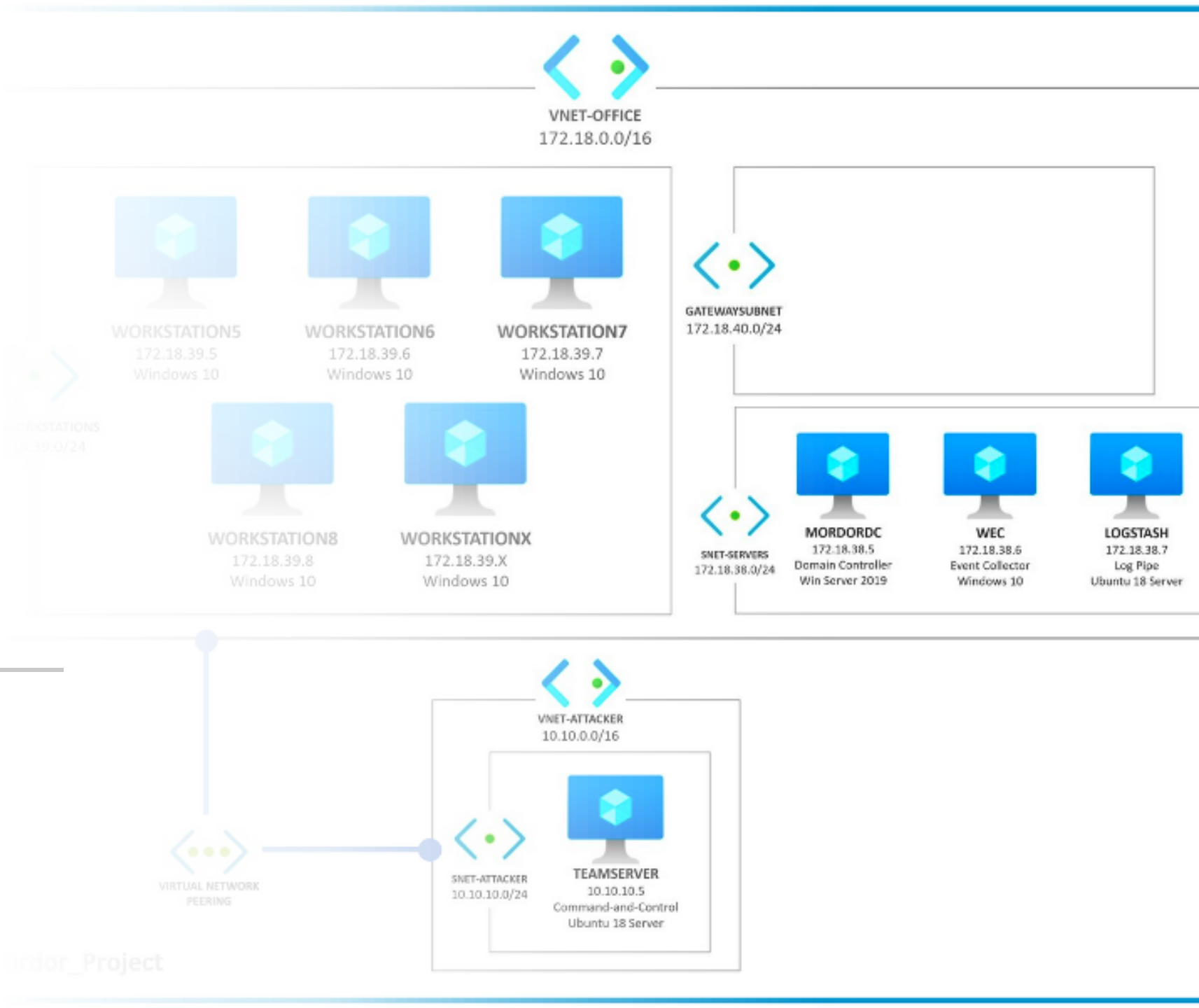
Varias tecnicas relacionadas
(Large datasets)

SCM and DLL Hijack IKEEXT

https://mordordatasets.com/notebooks/small/windows/03_persistence/SDWIN-190403133337.html

Diseño de Ambientes de Prueba

Desde Casa!



Usando el Proyecto SimuLand

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

Ambientes: ATT&CK Evaluations

ATT&CK Evaluations

APT29 Evaluations

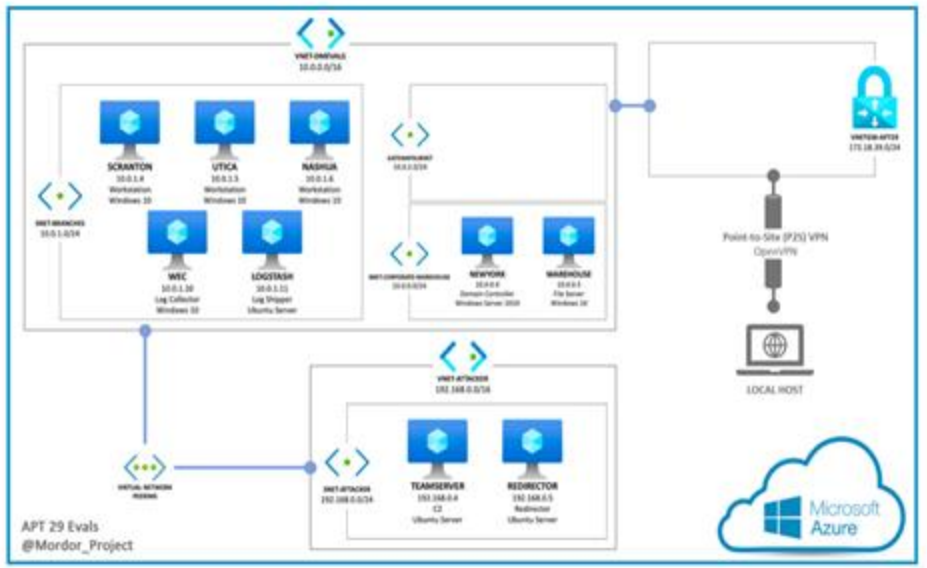
Deploy to Azure | Visualize

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

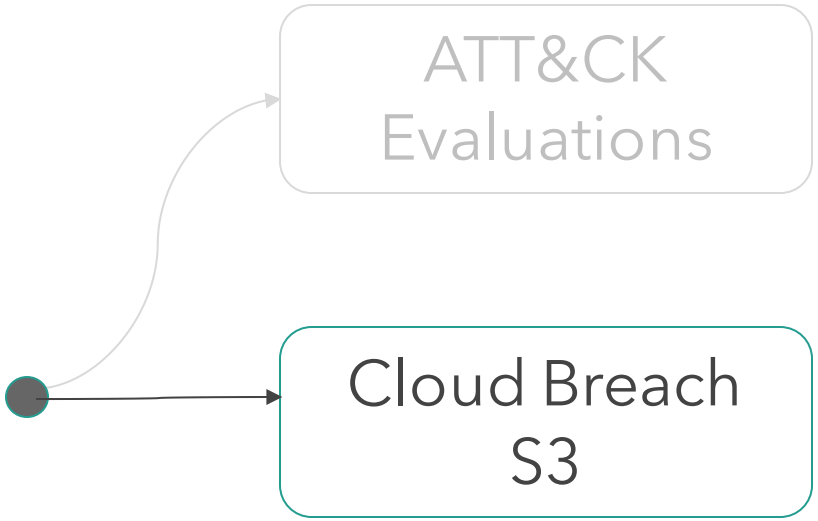
https://medium.com/threat-OTRF/mordor-labs-part-1-deploying-att-ck-apt29-evals-environments-via-arm-templates-to-create-1c6c4bc32c9a

Network Design



https://github.com/OTRF/SimuLand/tree/master/environments/attack-evals/apt29

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: cloudtrail
  - Kafkacat
    - Ready to consume logs from kafka

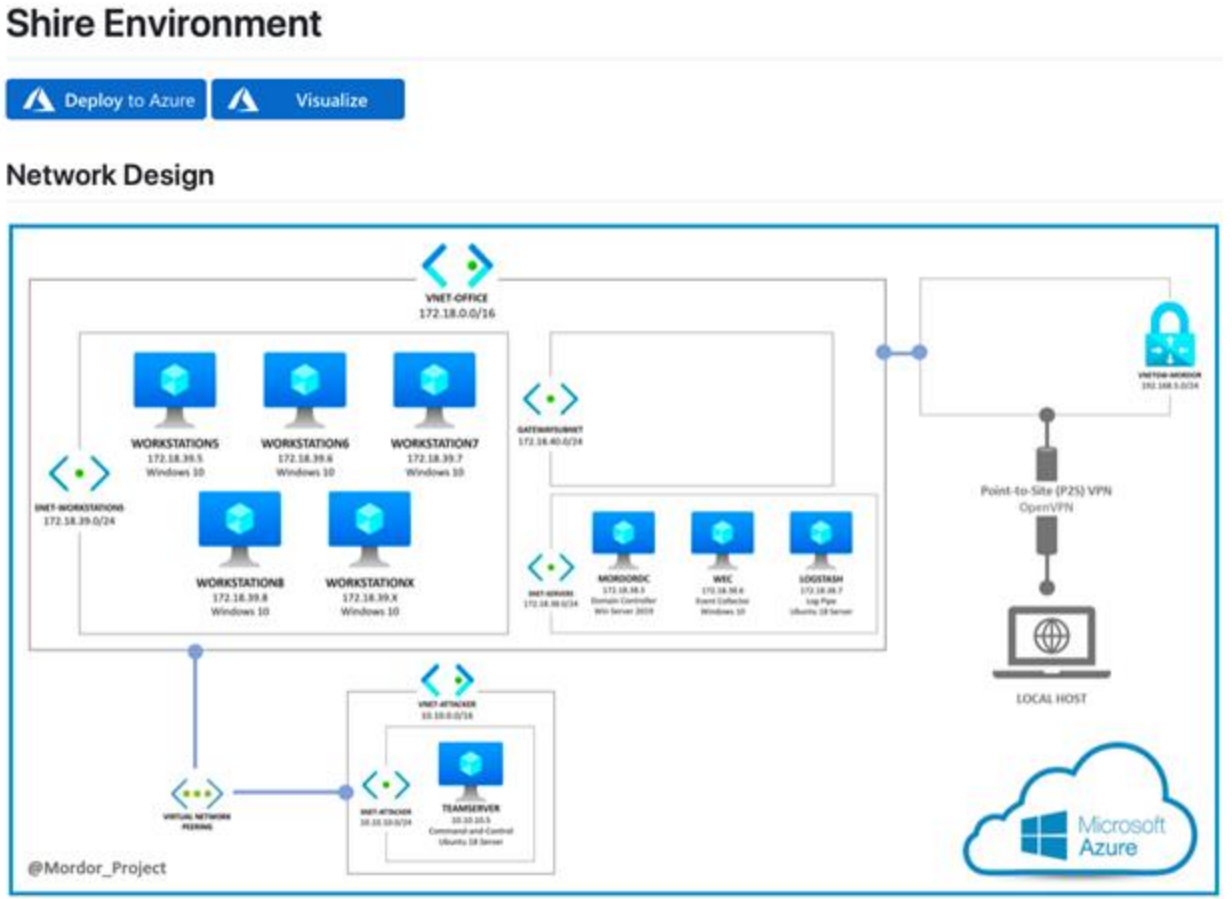
https://github.com/OTRF/SimuLand/tree/master/environments/aws/cloud-breach-s3

Ambientes: The Shire

ATT&CK Evaluations

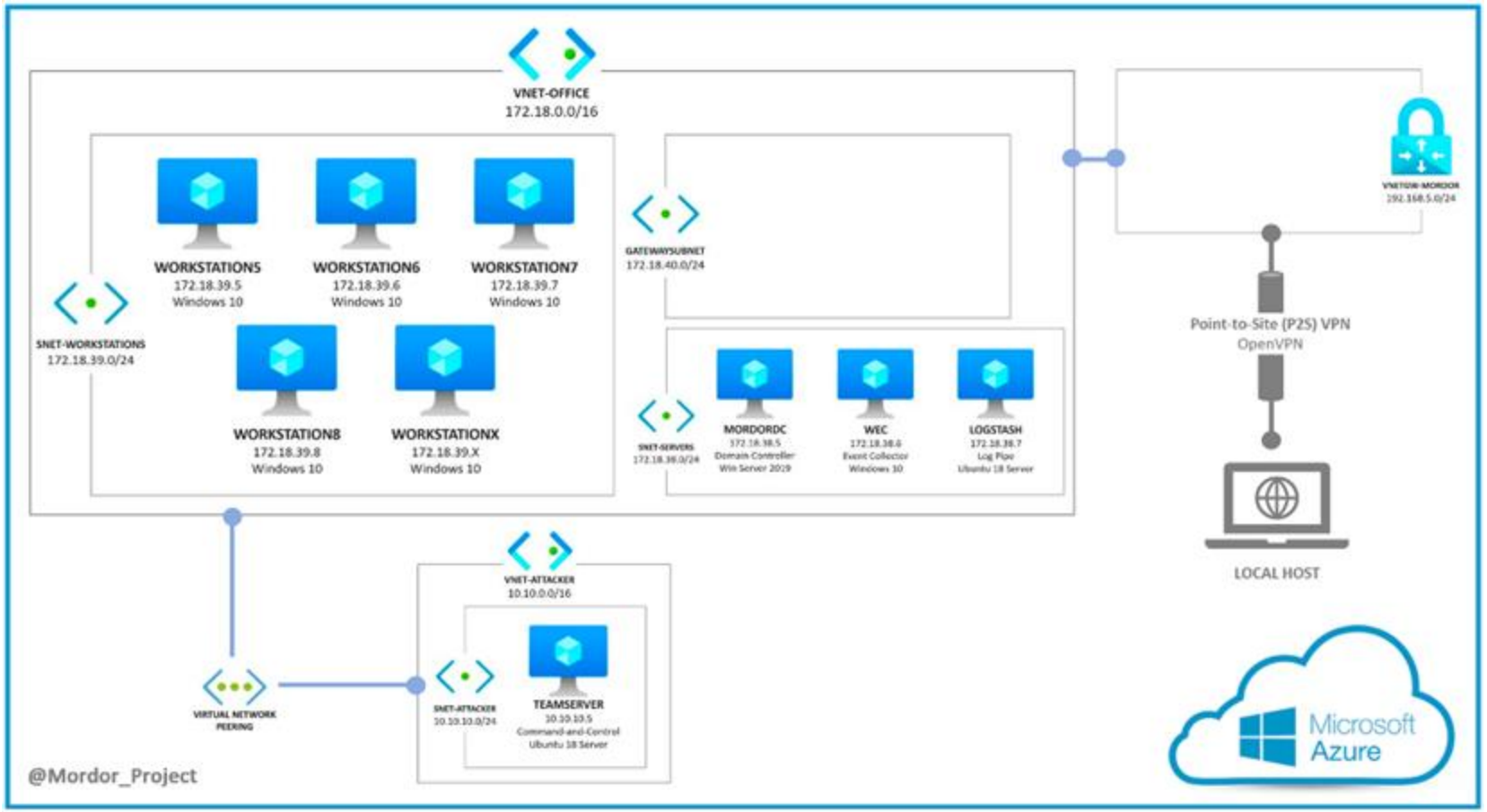
Cloud Breach S3

The Shire



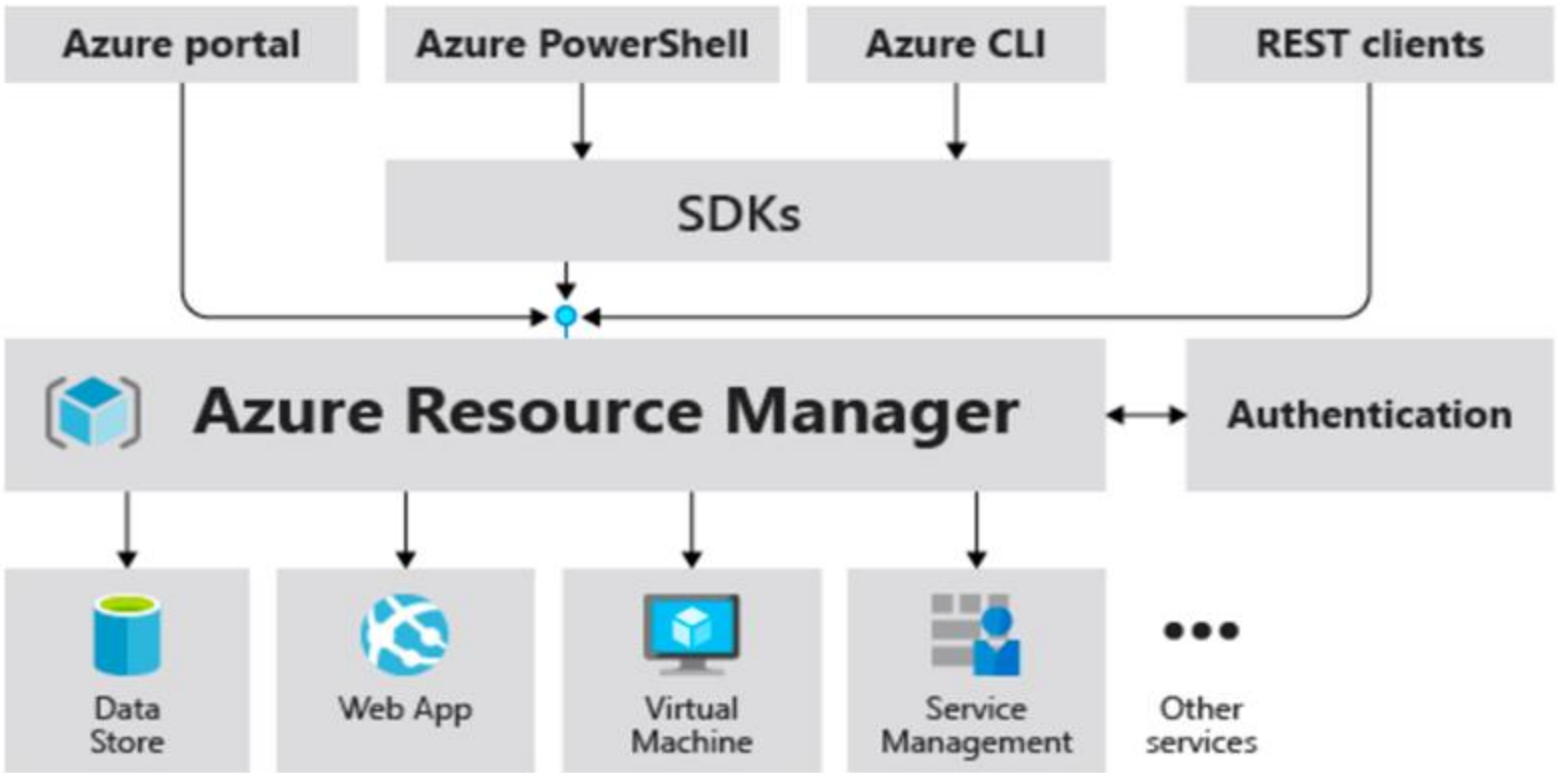
https://github.com/OTRF/SimuLand/tree/master/environments/windows/shire

The Shire (Windows)



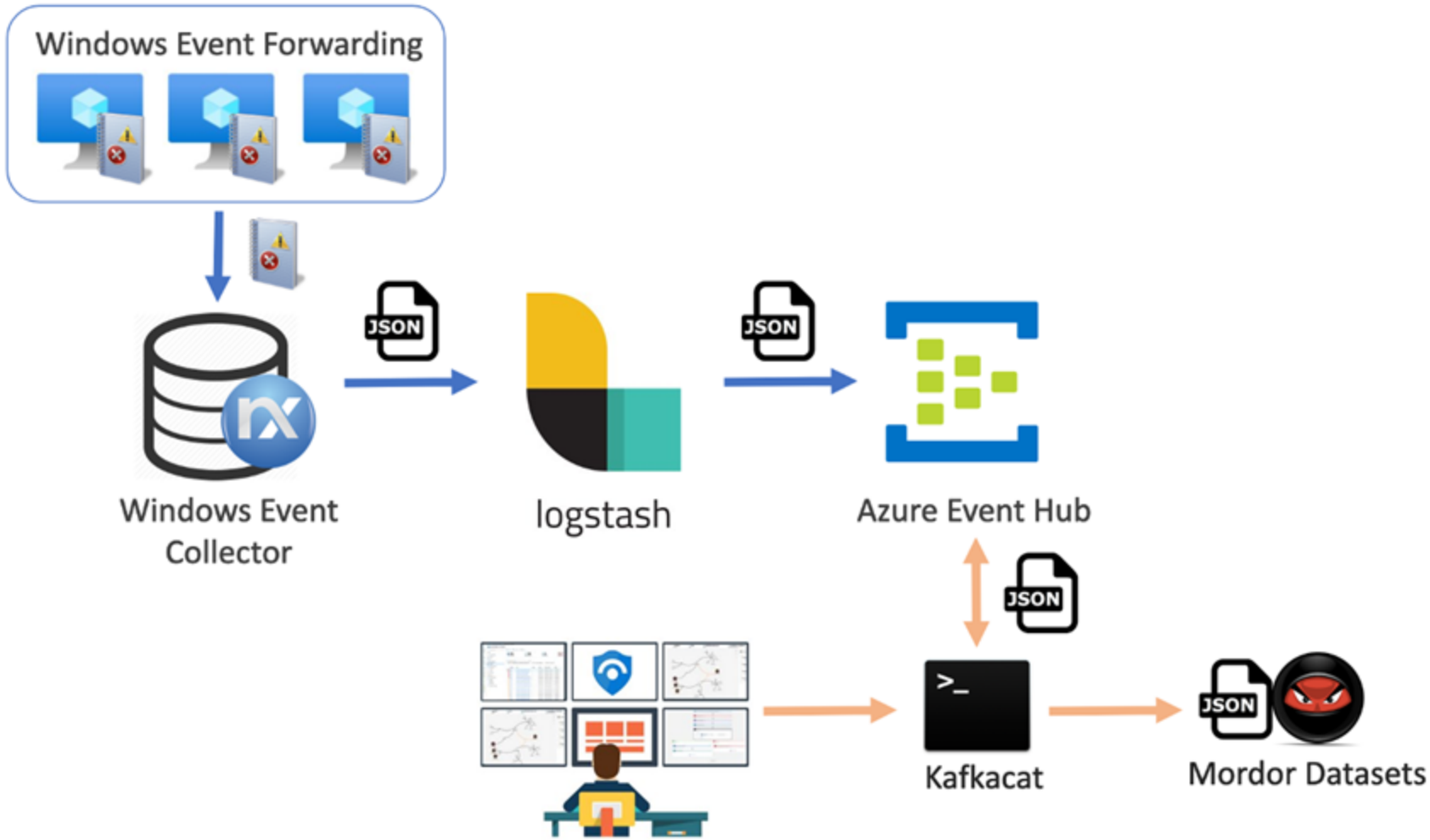
https://github.com/OTRF/SimuLand/tree/master/environments/windows/shire

Servicio de Azure Resource Manager



https://github.com/OTRF/SimuLand/tree/master/environments/windows/shire

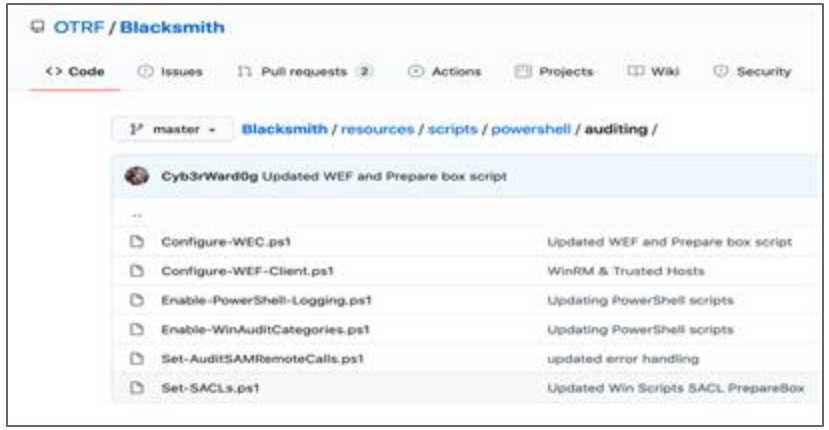
Coleccionando Data!



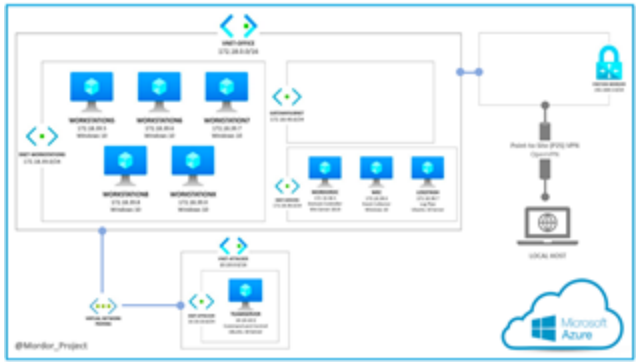
https://github.com/OTRF/SimuLand/tree/master/environments/windows/shire

https://github.com/OTRF

Blacksmith

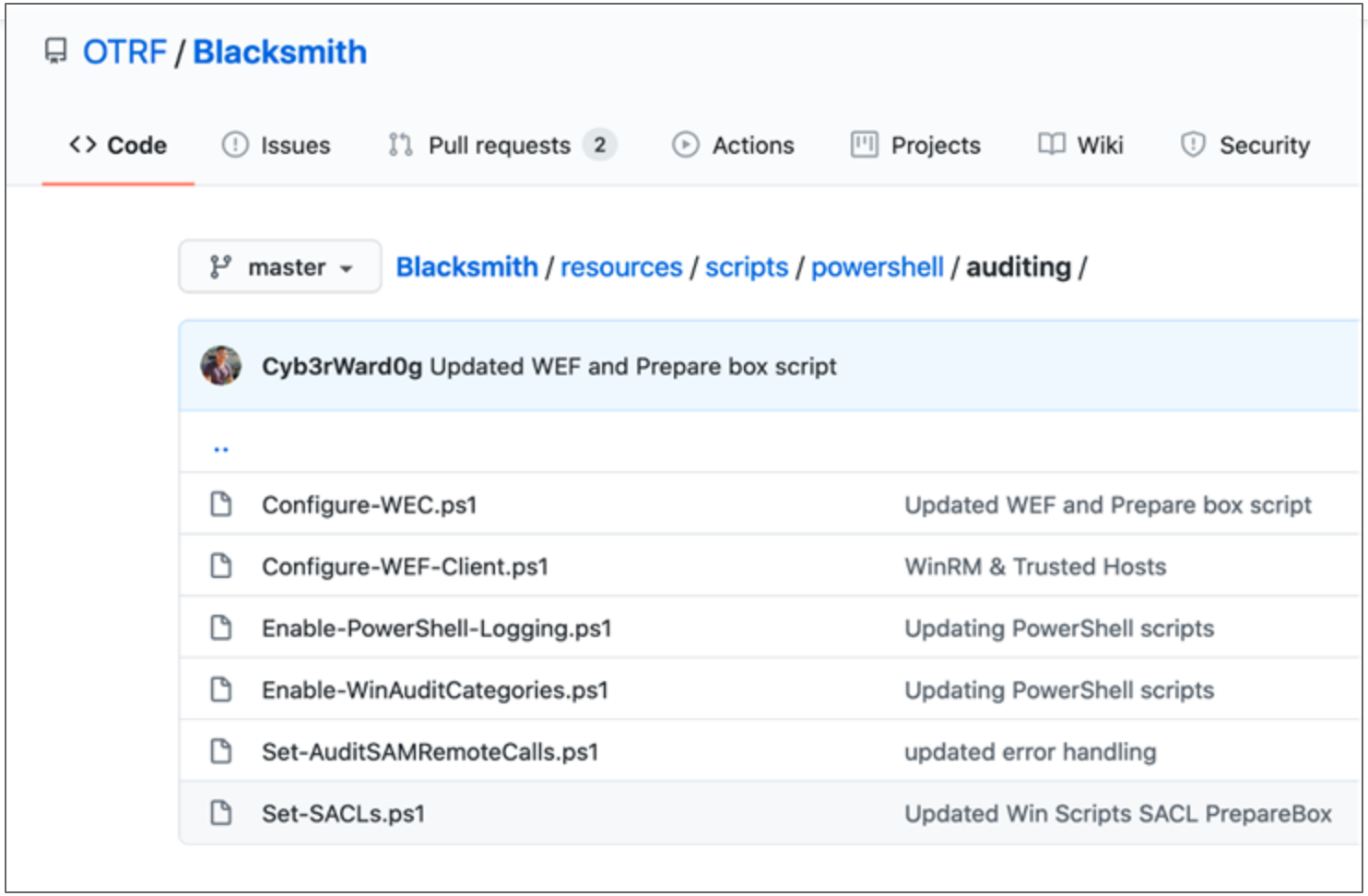


SimuLand



Mordor

Configurando Sistemas y Auditoria de Eventos



https://github.com/OTRF/SimuLand/tree/master/environments/windows/shire

Configurando PowerShell Logging

21 lines (19 sloc) | 918 Bytes

```
# Author: Roberto Rodriguez (@Cyb3rWard0g)
# License: GPL-3.0

# Enable PowerShell Logging
$regConfig = @"
regKey,name,value,type
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging","EnableScriptBlockLogging",1,"DWORD"
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging","EnableScriptBlockInvocationLogging",1,"DWORD"
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging","EnableModuleLogging",1,"DWORD"
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames",*,*,"String"
"@

Write-host "Setting up PowerShell registry settings.."
$regConfig | ConvertFrom-Csv | ForEach-Object {
    if(!(Test-Path $_.regKey)){
        Write-Host $_.regKey " does not exist.."
        New-Item $_.regKey -Force
    }
    Write-Host "Setting " $_.regKey
    New-ItemProperty -Path $_.regKey -Name $_.name -Value $_.value -PropertyType $_.type -force
}
```

https://github.com/OTRF/Blacksmith/blob/master/resources/scripts/powershell/auditing/Enable-PowerShell-Logging.ps1

Reglas de Auditoria para el Registro

```
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\JD";"Everyone";"QueryValues";"None";"None";"Success"
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Skew1";"Everyone";"QueryValues";"None";"None";"Success"
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\GBG";"Everyone";"QueryValues";"None";"None";"Success"
"HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Data";"Everyone";"QueryValues";"None";"None";"Success"
"@

write-host "Enabling audit rules.."
$AuditRules | ConvertFrom-Csv -Delimiter ';' | ForEach-Object {
    if(!(Test-Path $_.regKey)){
        Write-Host $_.regKey " does not exist.."
    }
    else {
        Write-Host "Updating SACL of " $_.regKey
        Set-AuditRule -RegistryPath $_.regKey -IdentityReference $_.identityReference  -Rights $_.rights.split(",")
    }
}
```

https://github.com/OTRF/Blacksmith/blob/master/resources/scripts/powershell/auditing/Set-SACLs.ps1

Reglas de Auditoria para Servicios 

```powershell
$ServiceRules = @"
service;addition
"IKEEXT";"(AU;SAFA;RPWPDTCCLC;;;WD)"
"SessionEnv";"S:(AU;SAFA;RPWPDTCCLC;;;WD)"
"scmanager";"(AU;SAFA;GA;;;NU)"
"@

$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"
    }
}
```

https://github.com/OTRF/Blacksmith/blob/master/resources/scripts/powershell/auditing/Set-SACLs.ps1

Reglas de Auditoria para Servicios 

```
68  $ServiceRules = @"
69  service;addition
70  "IKEEXT";"(AU;SAFA;RPWPDTCCLC;;;WD)"
71  "SessionEnv";"S:(AU;SAFA;RPWPDTCCLC;;;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  }
```

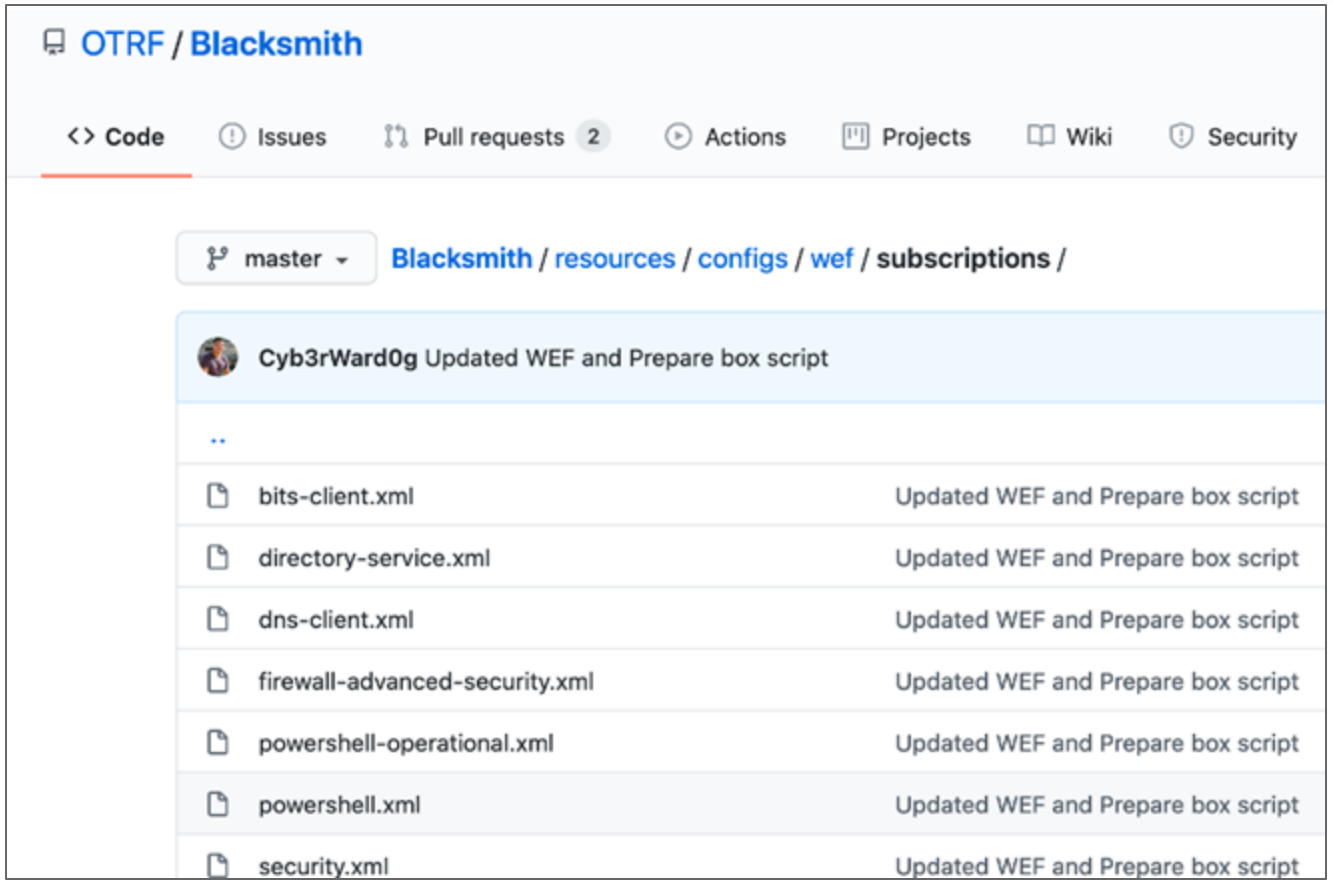
https://github.com/OTRF/Blacksmith/blob/master/resources/scripts/powershell/auditing/Set-SACLs.ps1

AU;SAFA;RPWPDTCCLC;;;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  #>
```

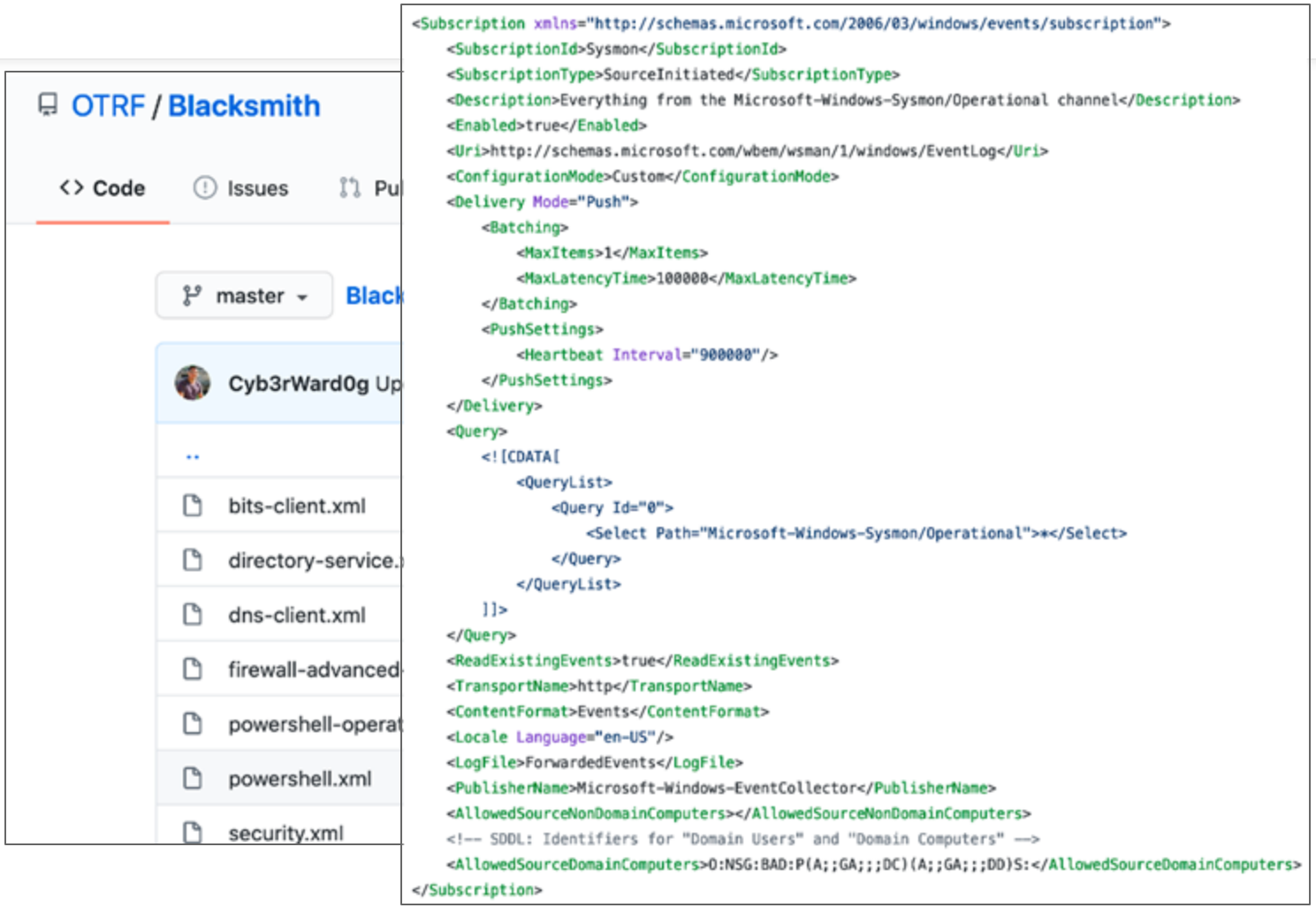
https://github.com/OTRF/Blacksmith/blob/master/resources/scripts/powershell/auditing/Set-SACLs.ps1

Windows Event Forwarding (WEF)



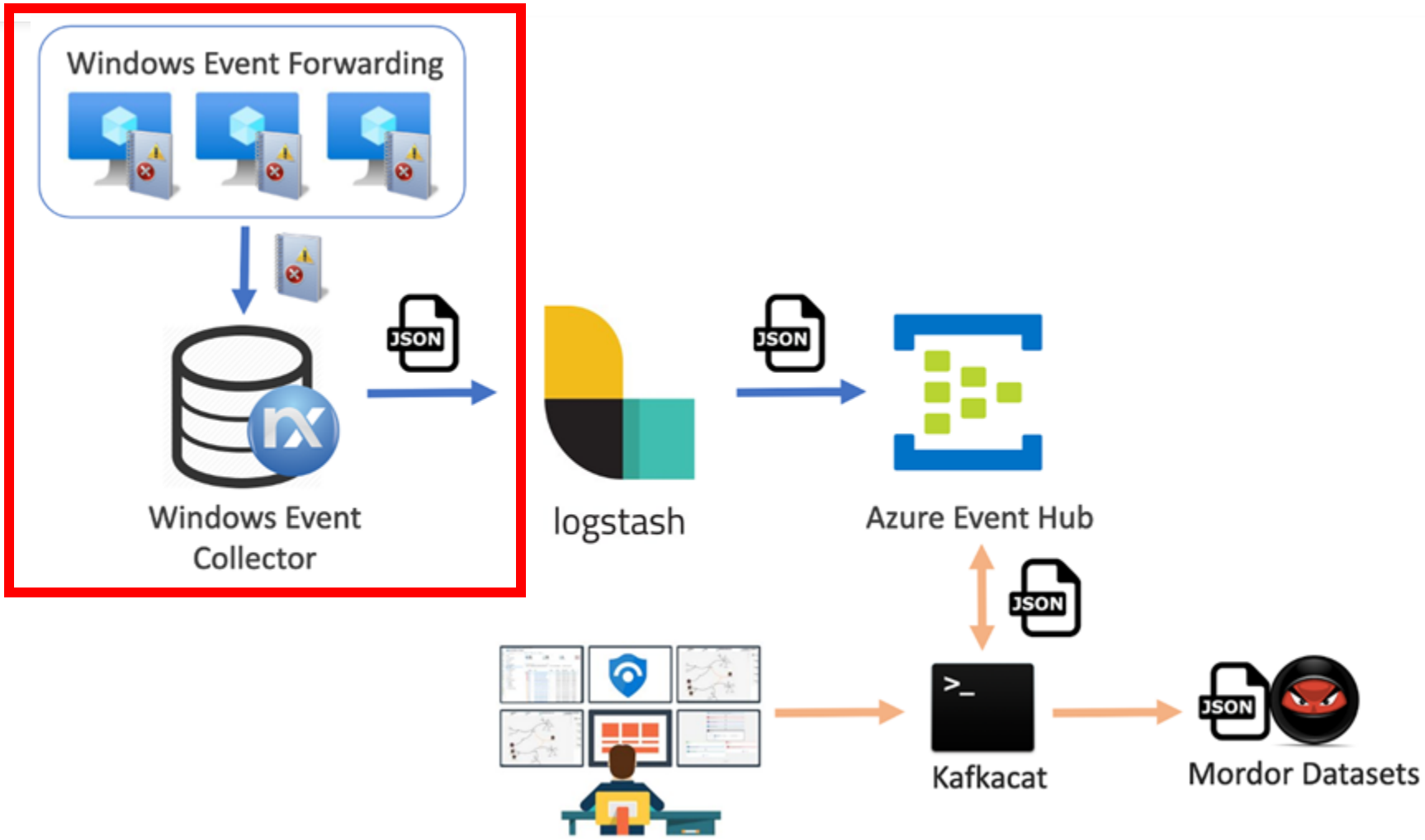
https://github.com/OTRF/Blacksmith/tree/master/resources/configs/wef/subscriptions

Windows Event Forwarding (WEF)

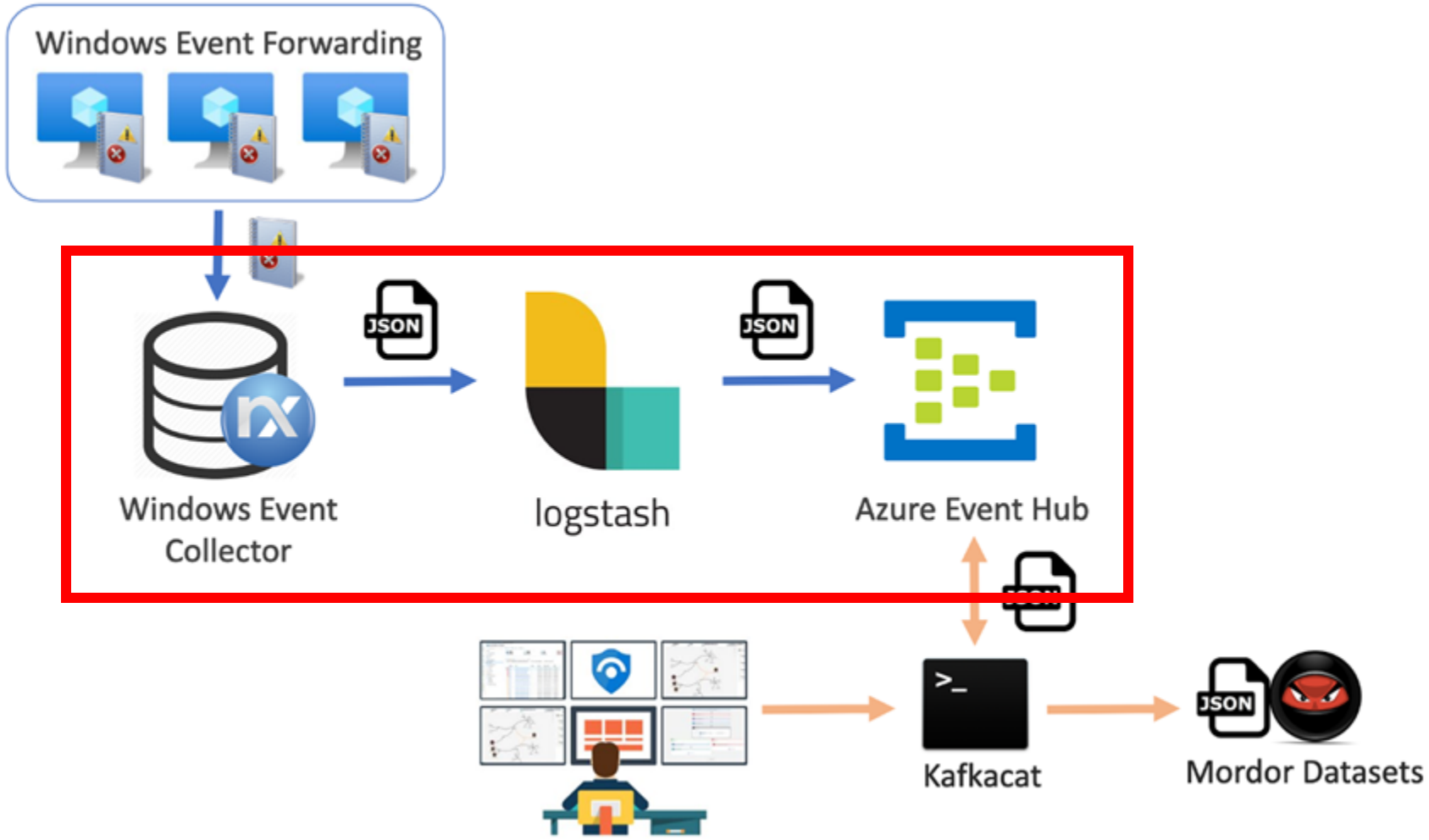


https://github.com/OTRF/Blacksmith/tree/master/resources/configs/wef/subscriptions

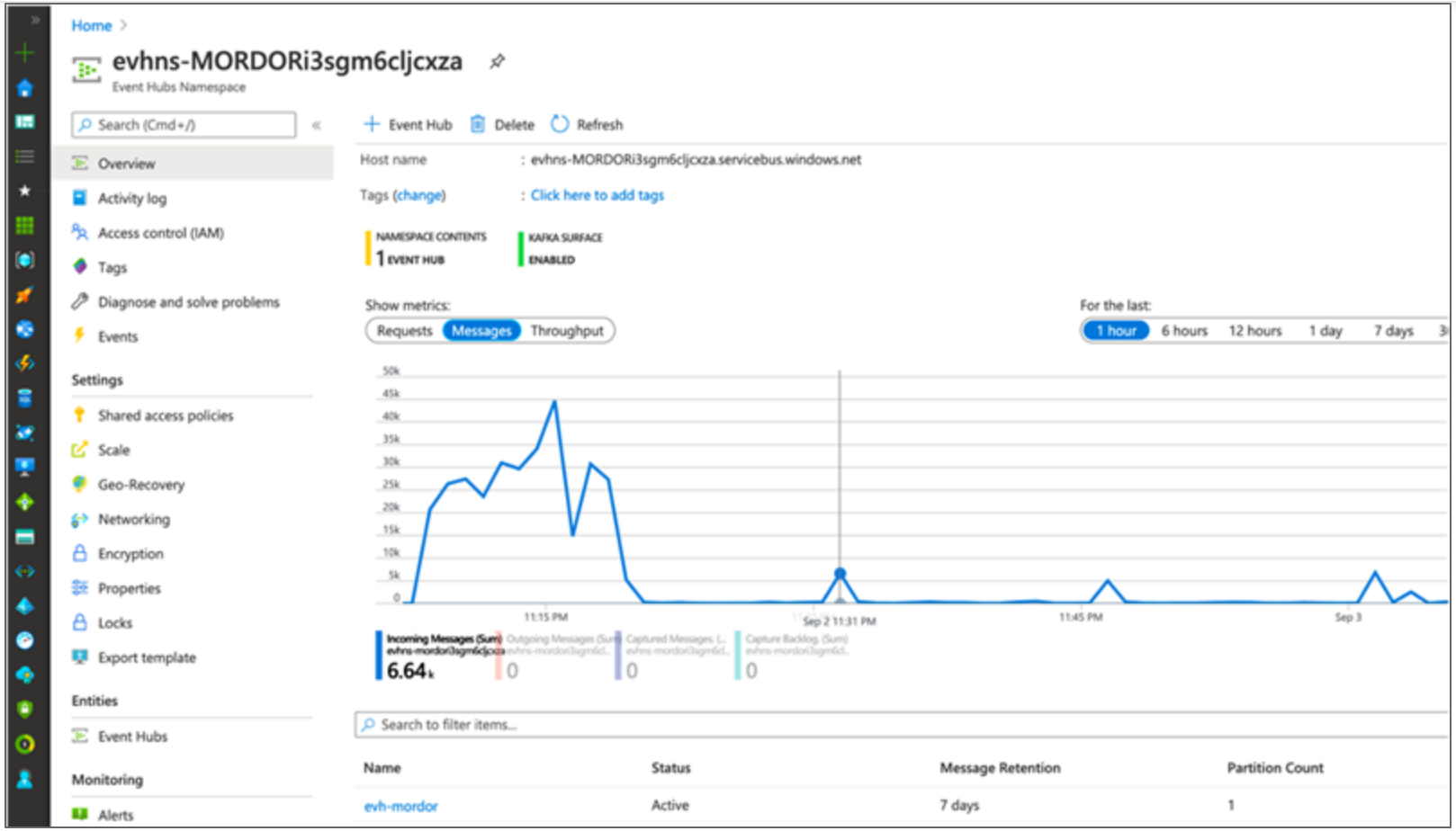
Todavia ni enviamos data..



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

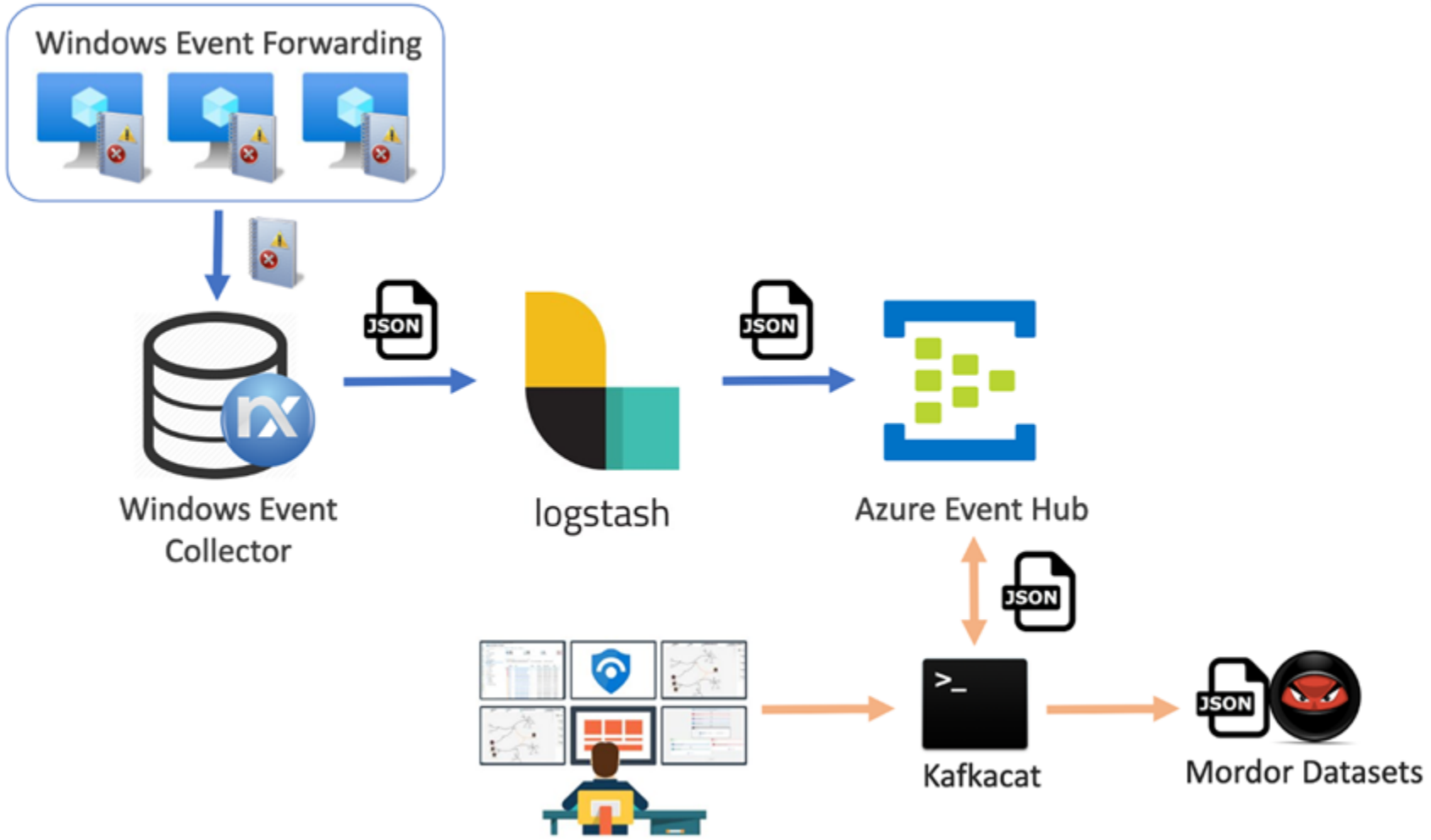


Azure Event Hub



https://azure.microsoft.com/en-us/services/event-hubs/

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.

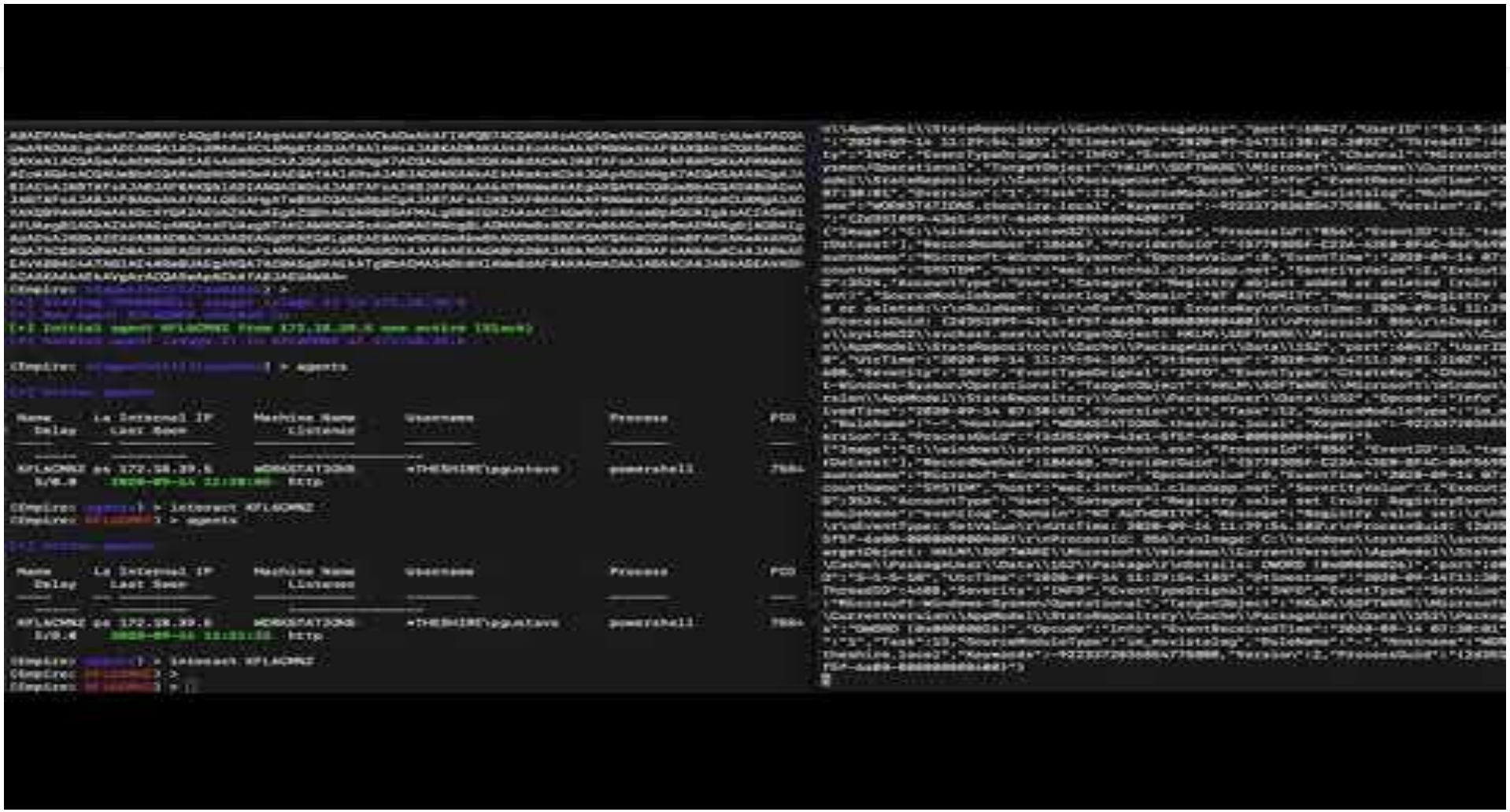
https://github.com/edenhill/kafkacat

Kafkacat: Modo Consumidor

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

https://github.com/edenhill/kafkacat

Kafkacat: Modo Consumidor

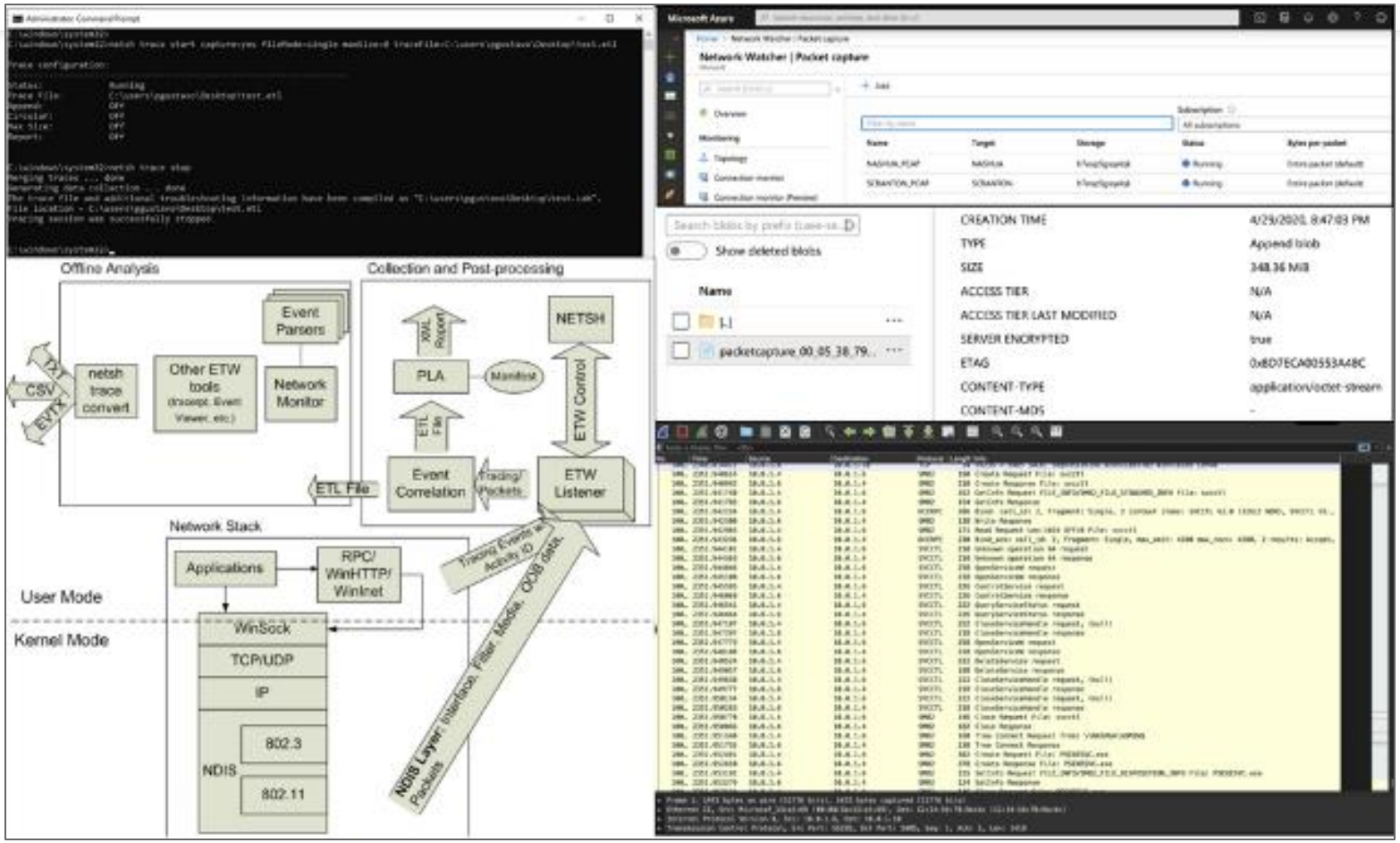


https://www.youtube.com/watch?v=x4STX5RlNJo

Kafkacat: Modo Consumidor

https://www.youtube.com/watch?v=xs6LsJ3QOEo

Y tambien capuras trafico de el network?



https://medium.com/threat-hunters-forge/mordor-pcaps-part-1-capturing-network-packets-from-windows-endpoints-with-network-shell-e117b84ec971

Network Shell (Windows ETW)

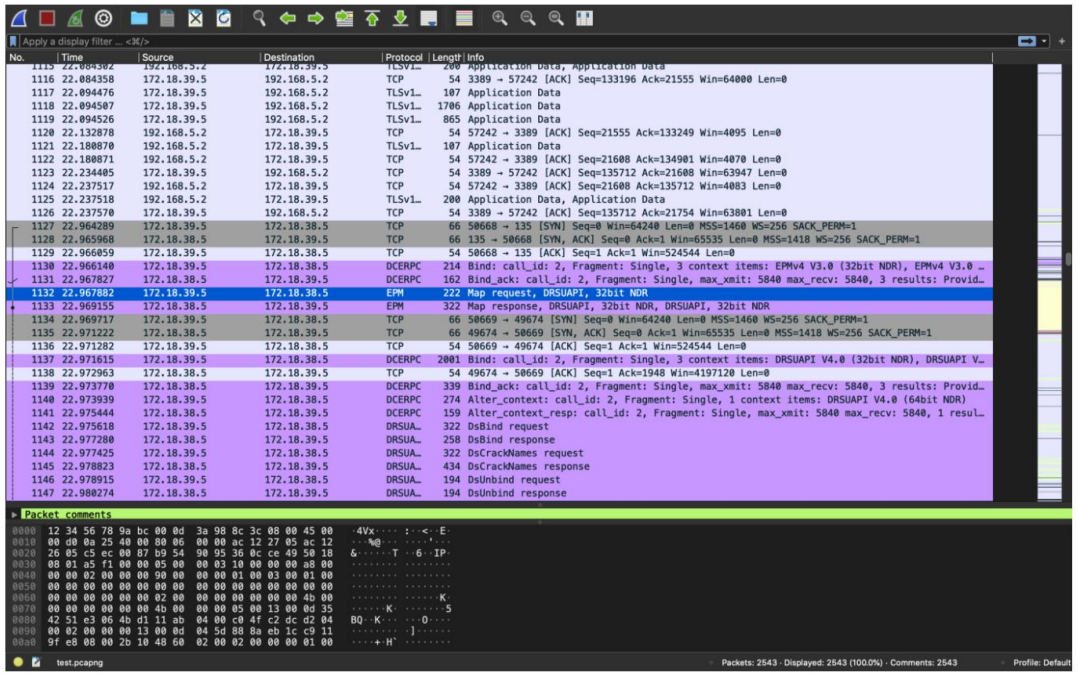
```
C:\>  netsh trace start capture=yes fileMode=single maxSize=0
traceFile=C:\users\pgustavo\Desktop\test.etl
```

- **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.

https://medium.com/threat-hunters-forge/mordor-pcaps-part-1-capturing-network-packets-from-windows-endpoints-with-network-shell-e117b84ec971

ETL2PCAPNG

```
etcl2pcapng.exe test.etl test.pcapng
```



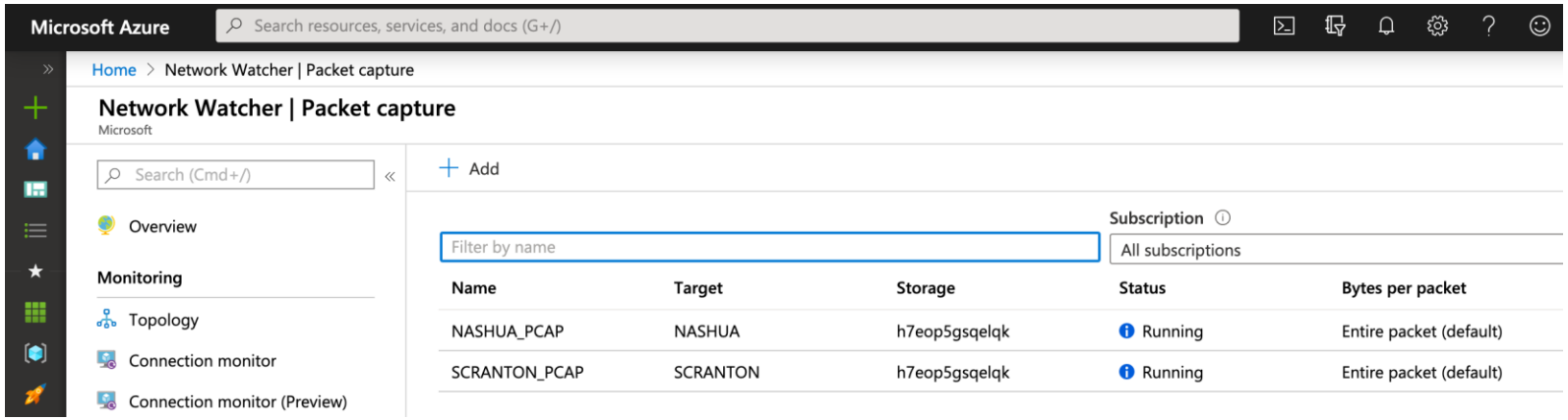
https://github.com/microsoft/etl2pcapng

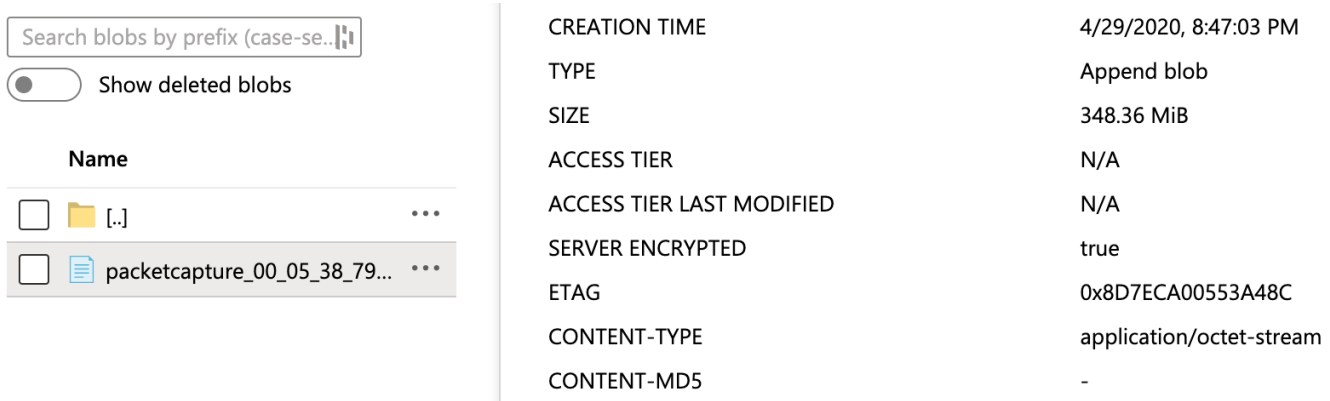
Azure Network Watcher (PCAPs)

```
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\"
 }
]
"
```

https://medium.com/threat-hunters-forge/mordor-pcaps-part-1-capturing-network-packets-from-windows-endpoints-with-network-shell-e117b84ec971

Azure Network Watcher (PCAPs)





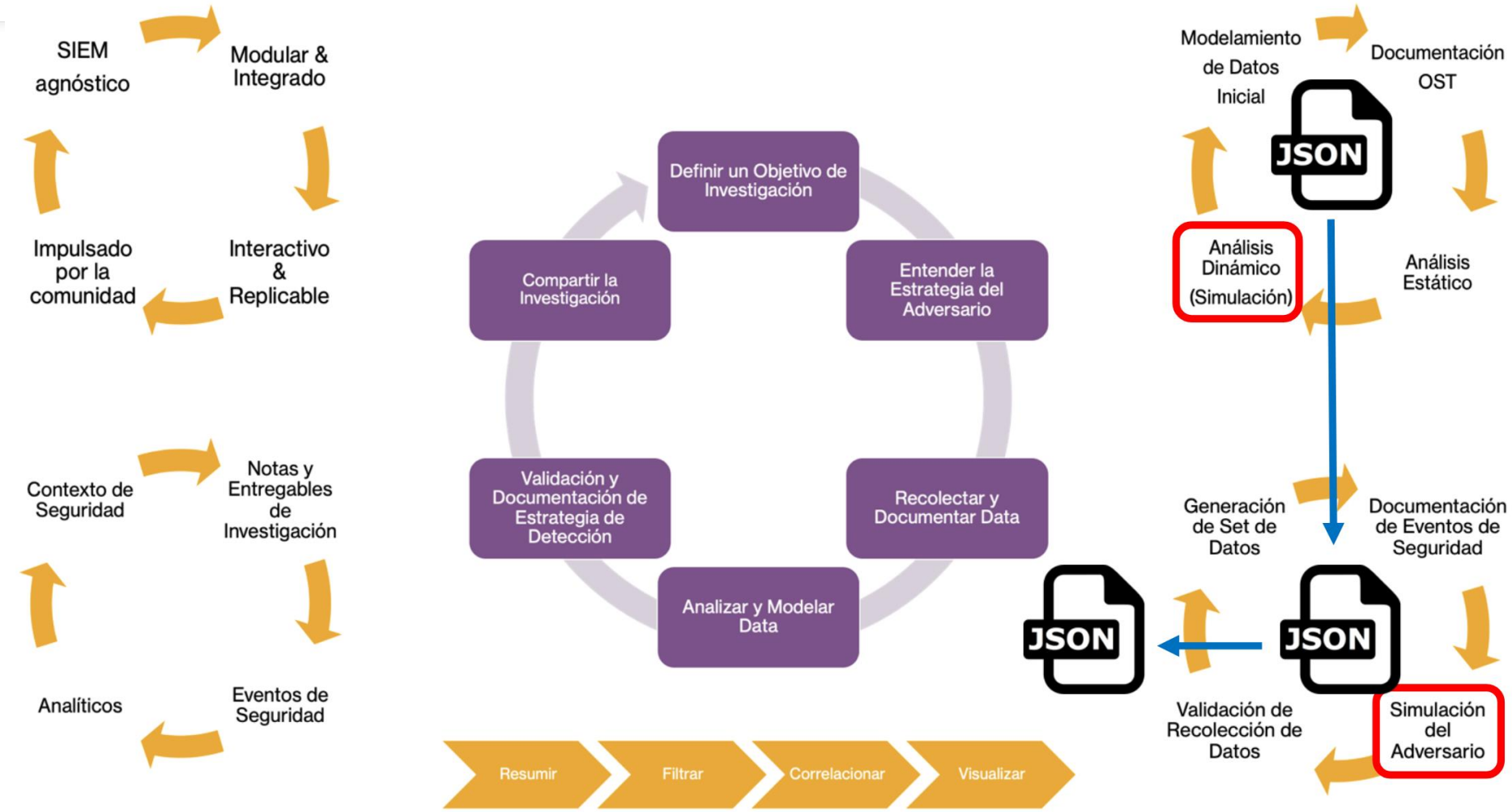
https://medium.com/threat-hunters-forge/mordor-pcaps-part-1-capturing-network-packets-from-windows-endpoints-with-network-shell-e117b84ec971

Qué podemos hacer con la data?

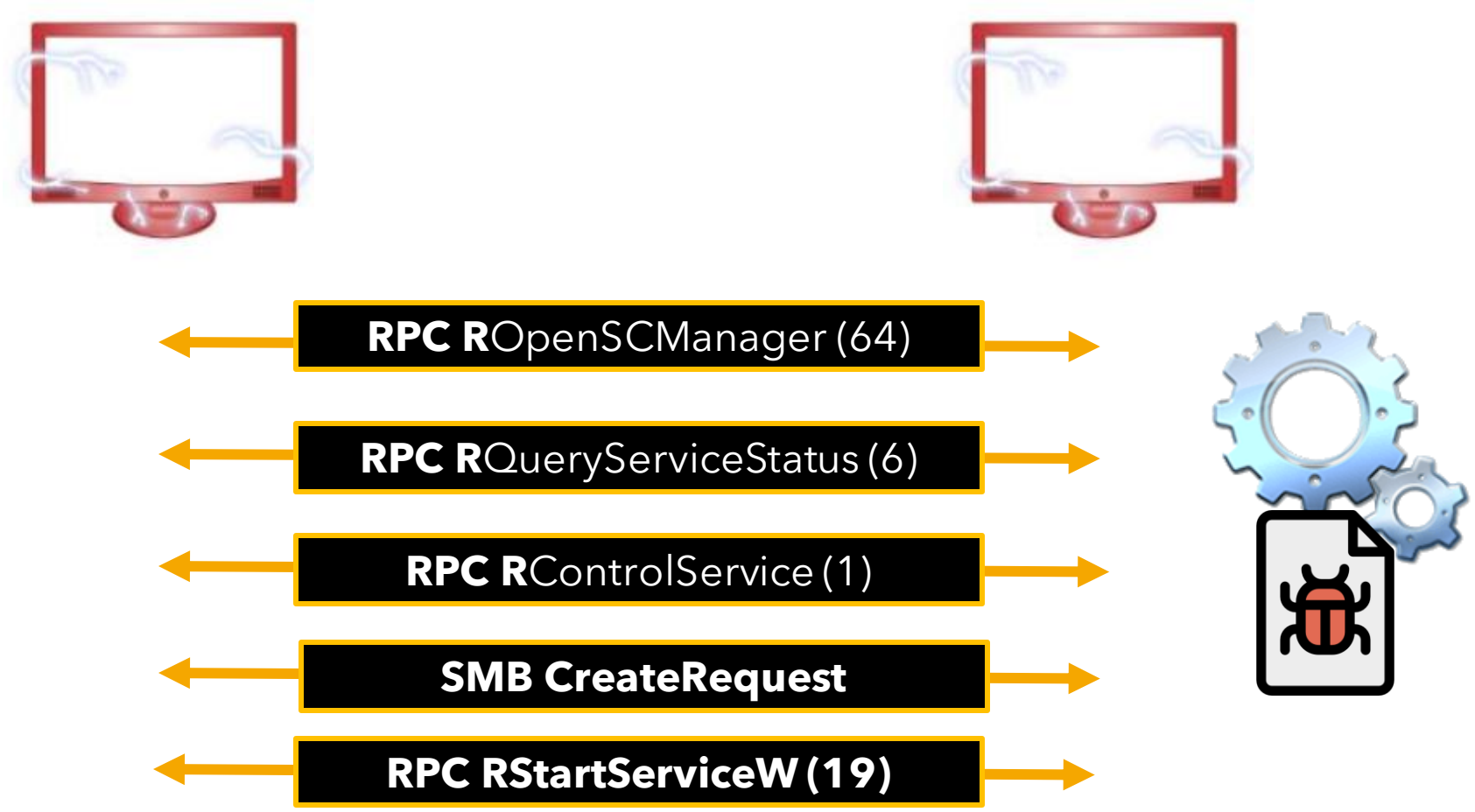
Mordor Files

- Entrenamiento de analistas de seguridad
- Entrevistas de trabajo
- Eventos (Hackathons)
- Validación de analiticos 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%'

''')
network_logon_excel.show(truncate = False, vertical=True)
```

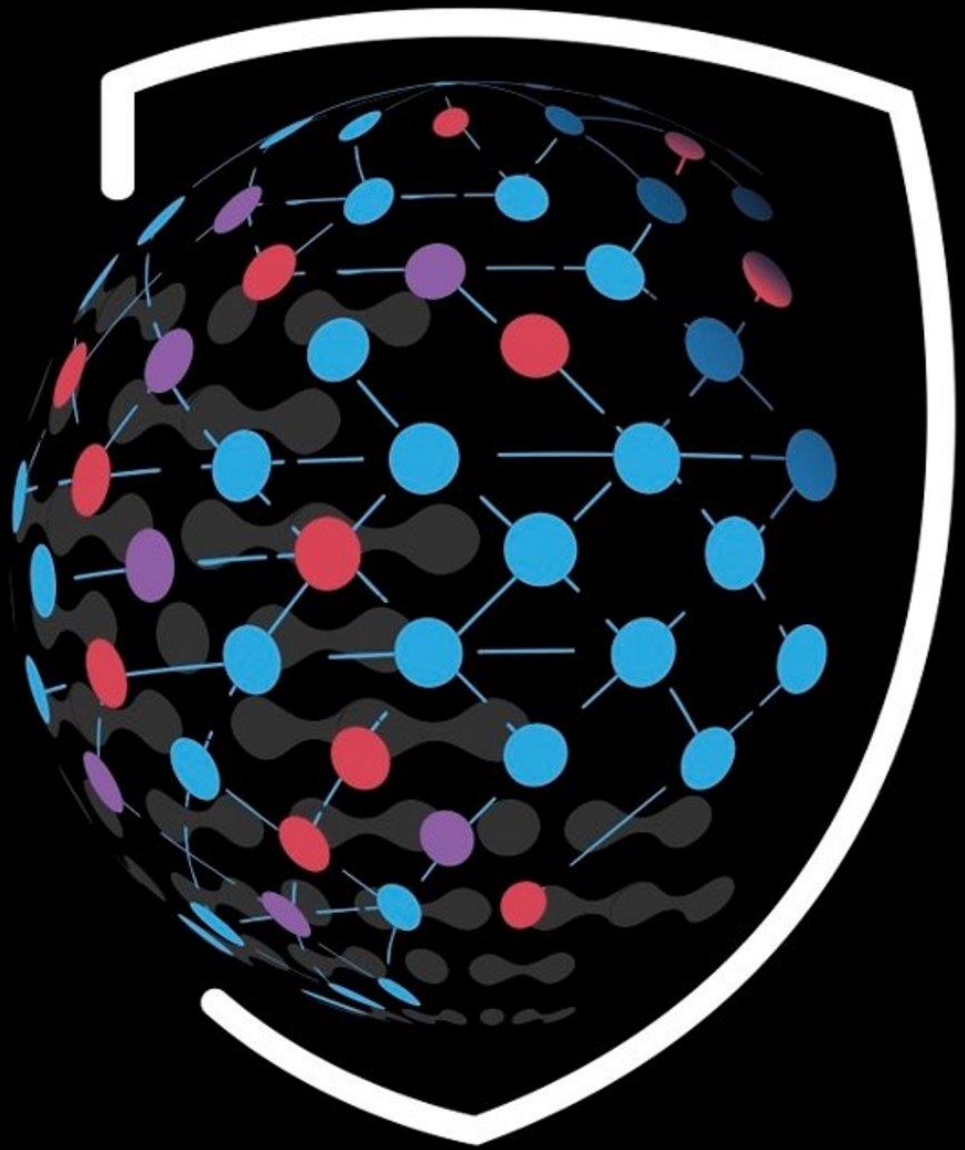
```
-RECORD 0-------------------------------------------------------------------------------------------------
 Hostname          | WORKSTATION6.theshire.local
 Image             | C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE
 ImageLoaded       | C:\ProgramData\calc.xll
 ParentCommandLine | 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 especifico
- 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 codigo de conducta de nuestro discord

Muchas Gracias!