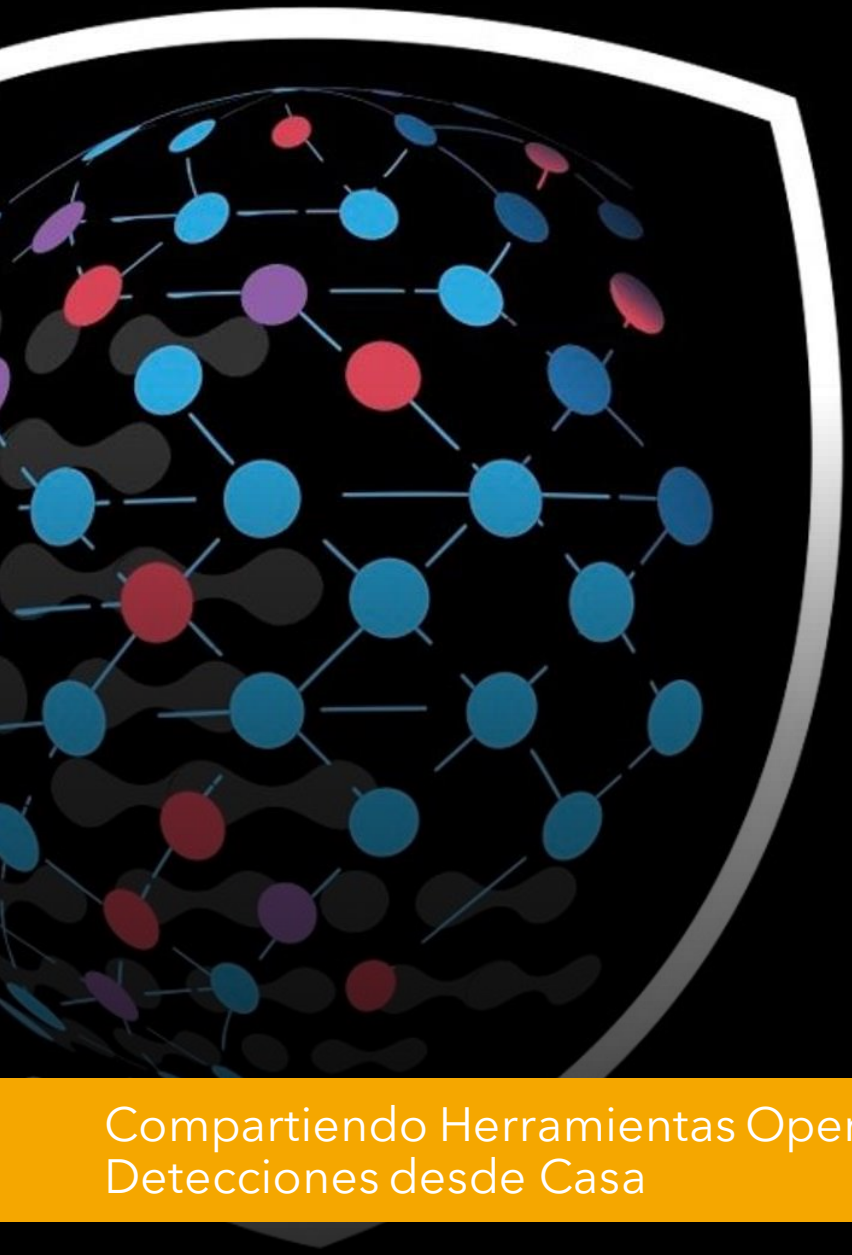


OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY

Compartiendo Herramientas Open Source con el Mundo para el desarrollo de Detecciones desde Casa

Quiénes Somos?

Amantes de la Colaboración y Fuente Abierta

Roberto Rodriguez 🇵🇪
@Cyb3rWard0g

- Microsoft Threat Intelligence Center (MSTIC)

Jose Rodriguez 🇵🇪
@Cyb3rPandaH

- MITRE - ATT&CK

- Colaboración Abierta ♡
- Threat Hunter Playbook @HunterPlaybook
- Mordor @Mordor_Project
- OSSEM @OSSEM_Project
- Blacksmith & more..

https://github.com/OTRF

Agenda

1) Qué Significa ser del lado Azul?
2) Una Metodología Basica
   - El Objetivo del R&D
   - Entendiendo al Adversario
   - Recolectando y Documentando Data
   - Analysis y Modelamiento de Datos
   - Validación y Documentación
   - Compartiendo con la Comunidad
3) Open Threat Research

Qué Significa ser del lado Azul?

Defensivo? Ofensivo?

El Lado Azul

- Constante adaptación y aprendizaje
- Entender al adversario y su comportamiento por medio de horas y horas de leer documentación y simulaciones
- Documentar y modelar data en relación a acciones ejecutadas por el adversario
- Planear estrategies de colección de data para tener mejor visibilidad
- Enteder el como mitigar amenazas en paralelo con el desarrollo de detecciones
- Entender el estado normal de una organización
- Responder a incidentes e identificar el alcanze de el impacto

El Lado Azul

- Constante adaptación y aprendizaje
- **Aceptar diversidad en la industria**
- Entender al adversario y su comportamiento por medio de horas y horas de leer documentación y simulaciones
- **Identificar oportunidades de colaboración y aprendizaje**
- Documentar y modelar data en relacion a acciones ejecutadas por el adversario
- Planear estrategies de colección de data para tener mejor visibilidad
- **Adoptar conceptos abiertos para facilitar contribución y aprendizaje**
- Enteder el como mitigar amenazas en paralelo con el desarrollo de detecciones
- Responder a incidentes e identificar el alcanze de el impacto
- **Compartir conocimientos para empoderar a otros en la comunidad**

Aceptar y Adoptar Diversidad …

Ingeniería Inversa

Análisis de Inteligencia

Análisis de Datos

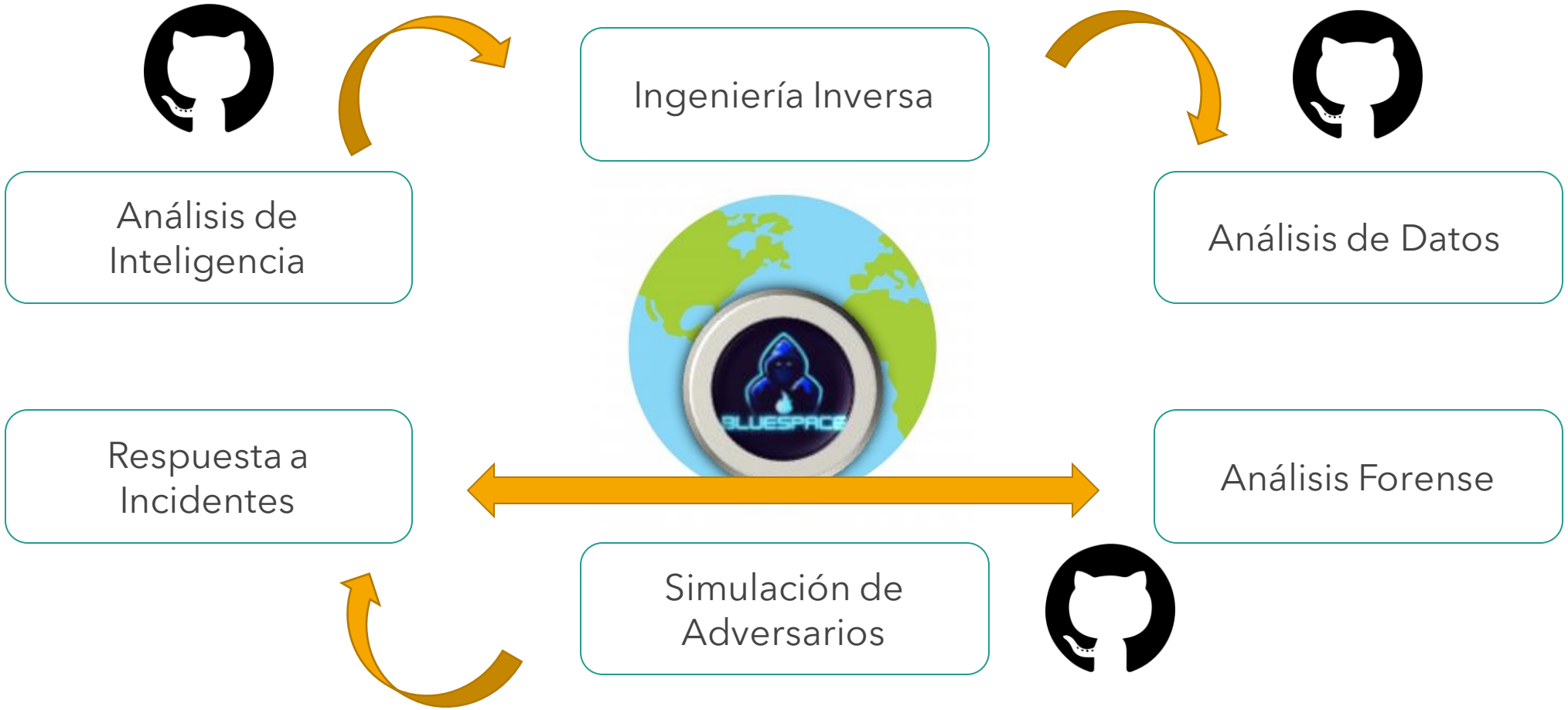
Respuesta a Incidentes

Análisis Forense

Simulación de Adversarios

Identificar Oportunidades de Collaboración

Adoptando Proyectos de Codigo Abierto



Compartir Conocimientos con la Comunidad

Colaboración en Conjunto

" If you want to go **fast**, go alone.
If you want to go **far**, go together"

African Proverb

Una Metodología Basica

Colaborando, desarrollando conceptos abiertos y compartiendo durante la investigacion y desarrollo de detecciones!


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

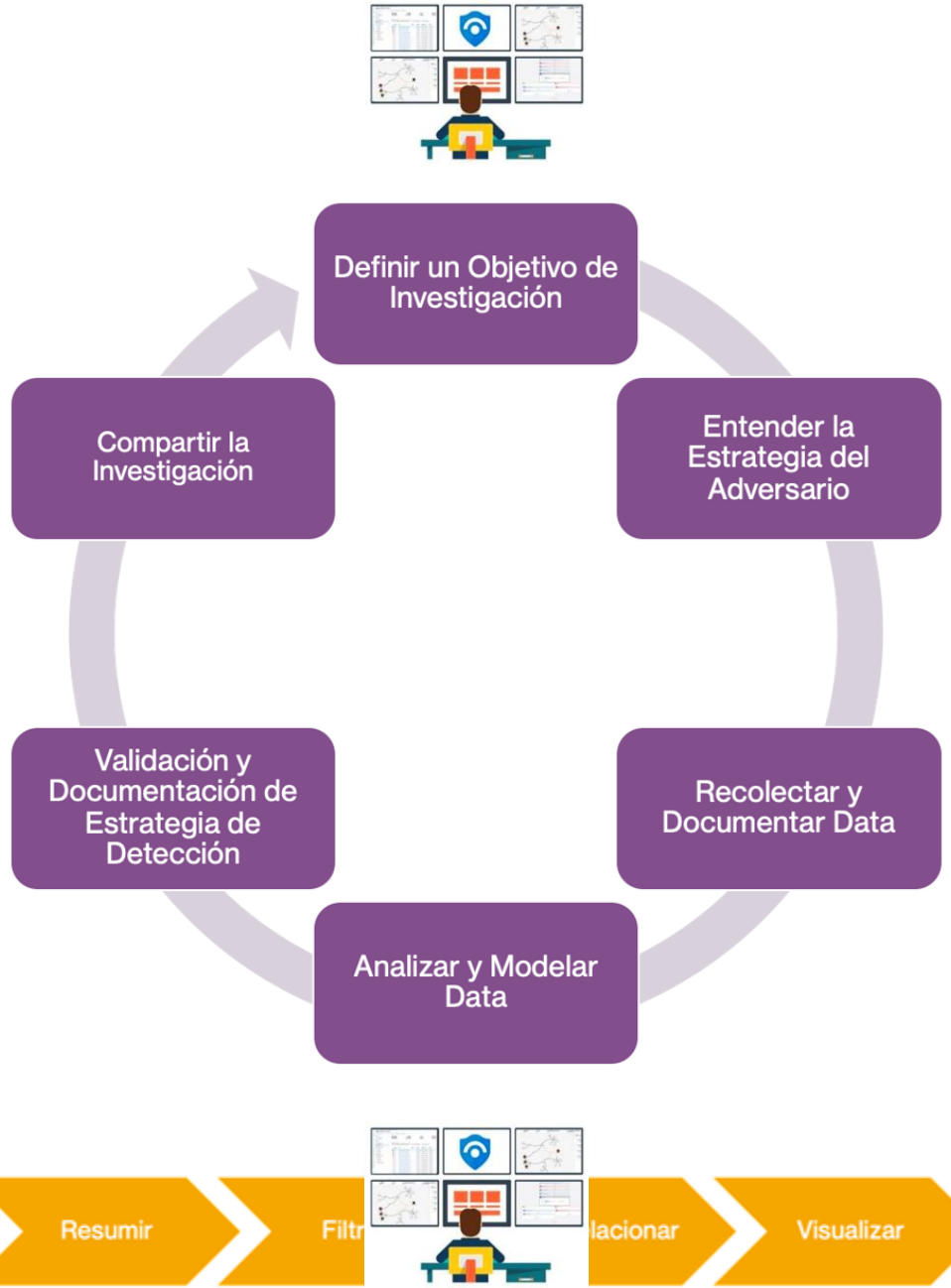

Modelamiento de Datos Inicial
Documentación OST
Análisis Estático
Análisis Dinámico (Simulación)

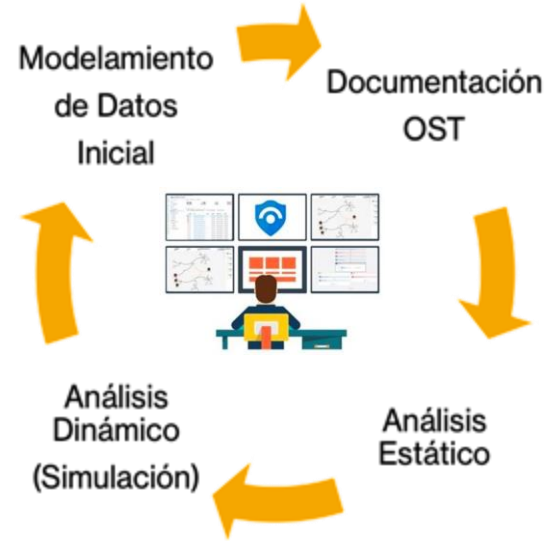

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Resumir
Filtrar
Correlacionar
Visualizar


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

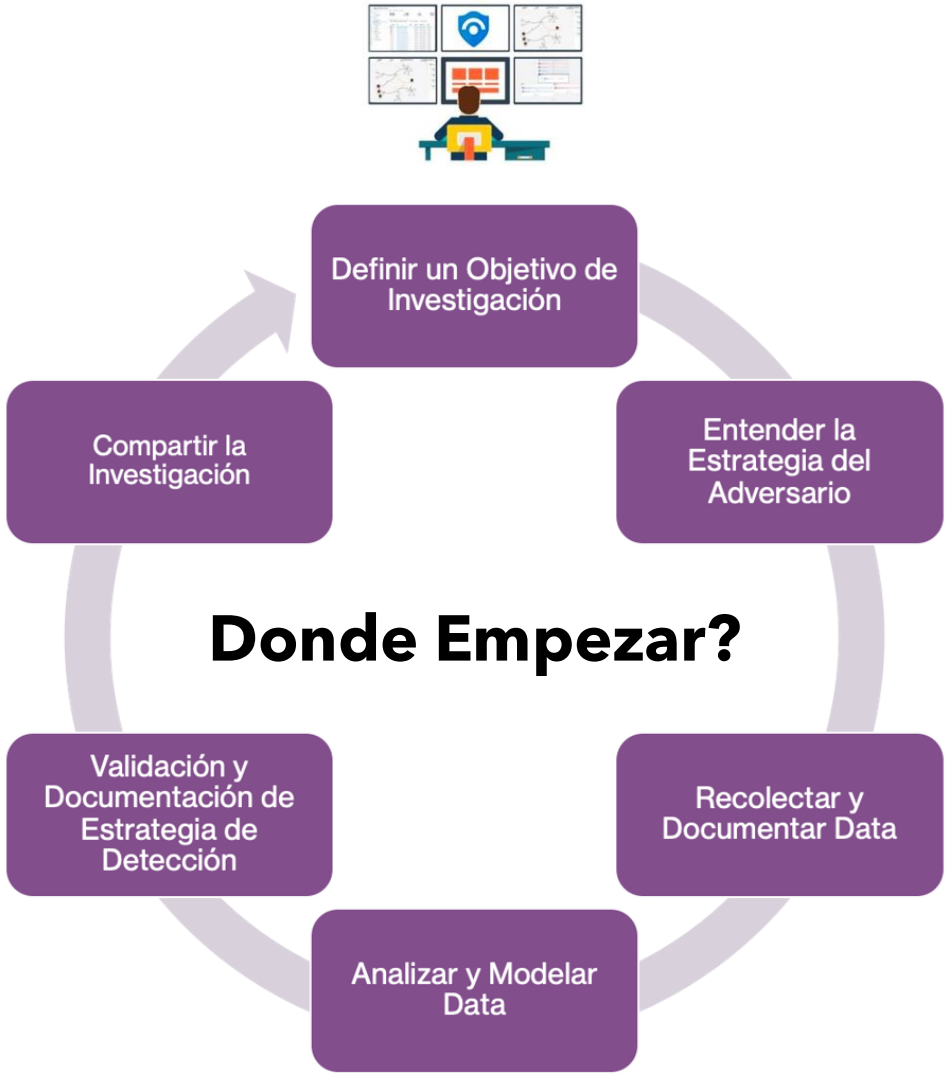

SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad


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
Visualizar


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

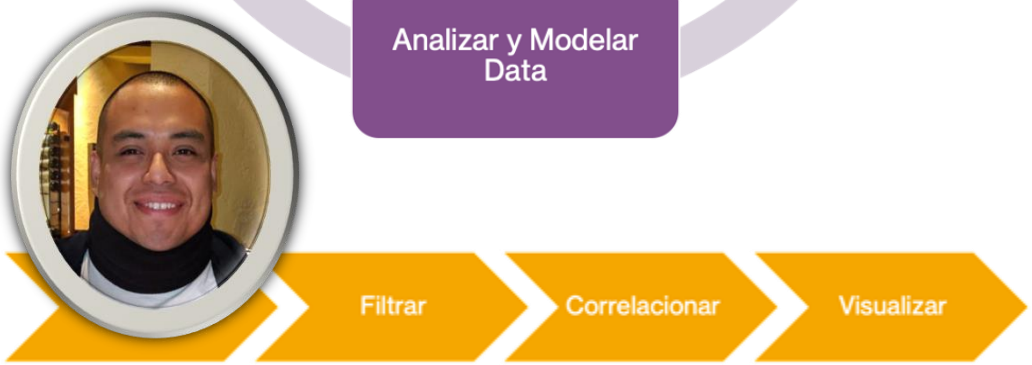

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


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



Donde Empezar?

Donde Empezar?



Dónde Empezar?

- 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

Filtrar → Correlacionar → Visualizar

Reconoce tus Fortalezas e Identifica tu Pasión

"Everybody is a Genius. But If You Judge a Fish by Its Ability to Climb a Tree, It Will Live Its Whole Life Believing that It is Stupid"

Albert Einstein


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)

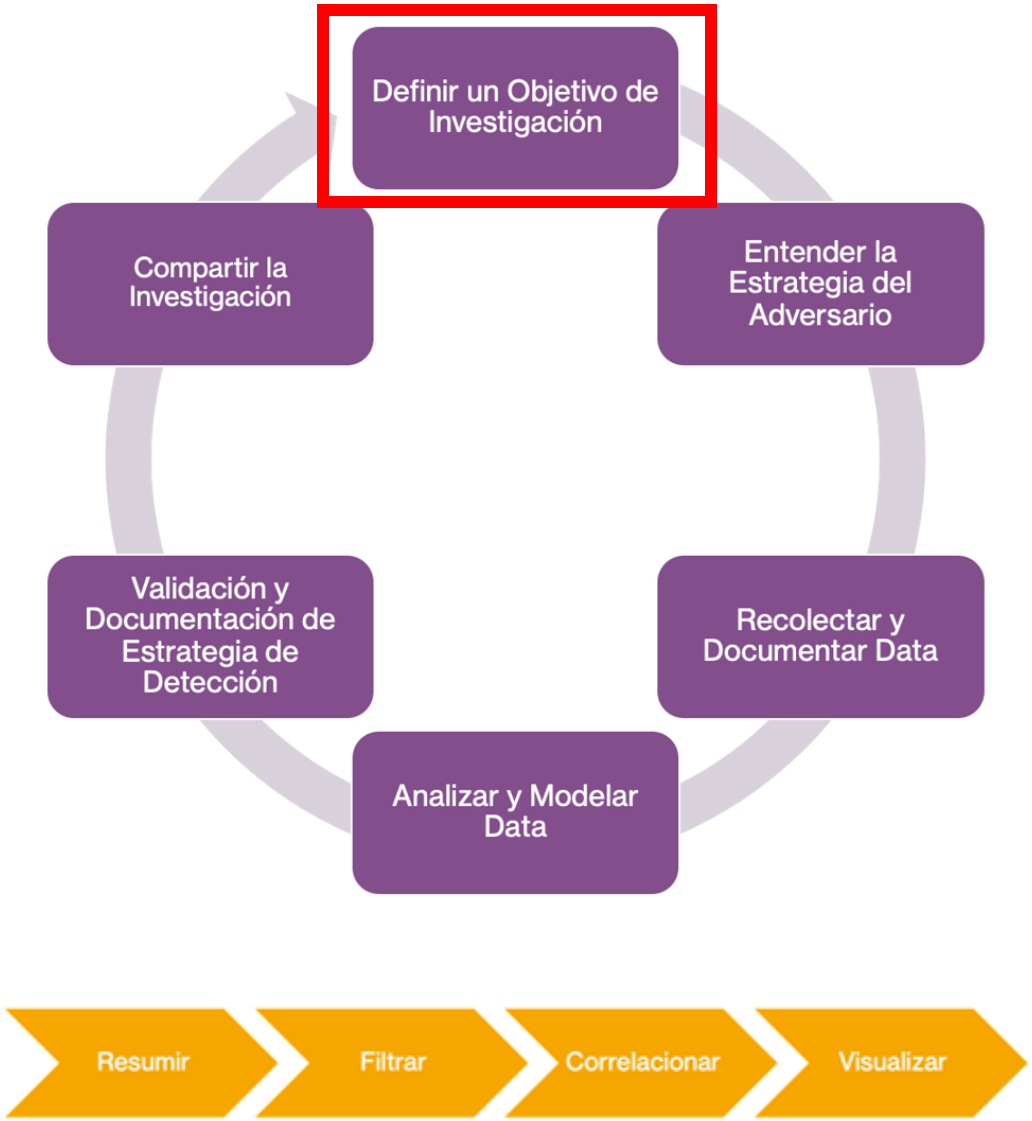

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


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

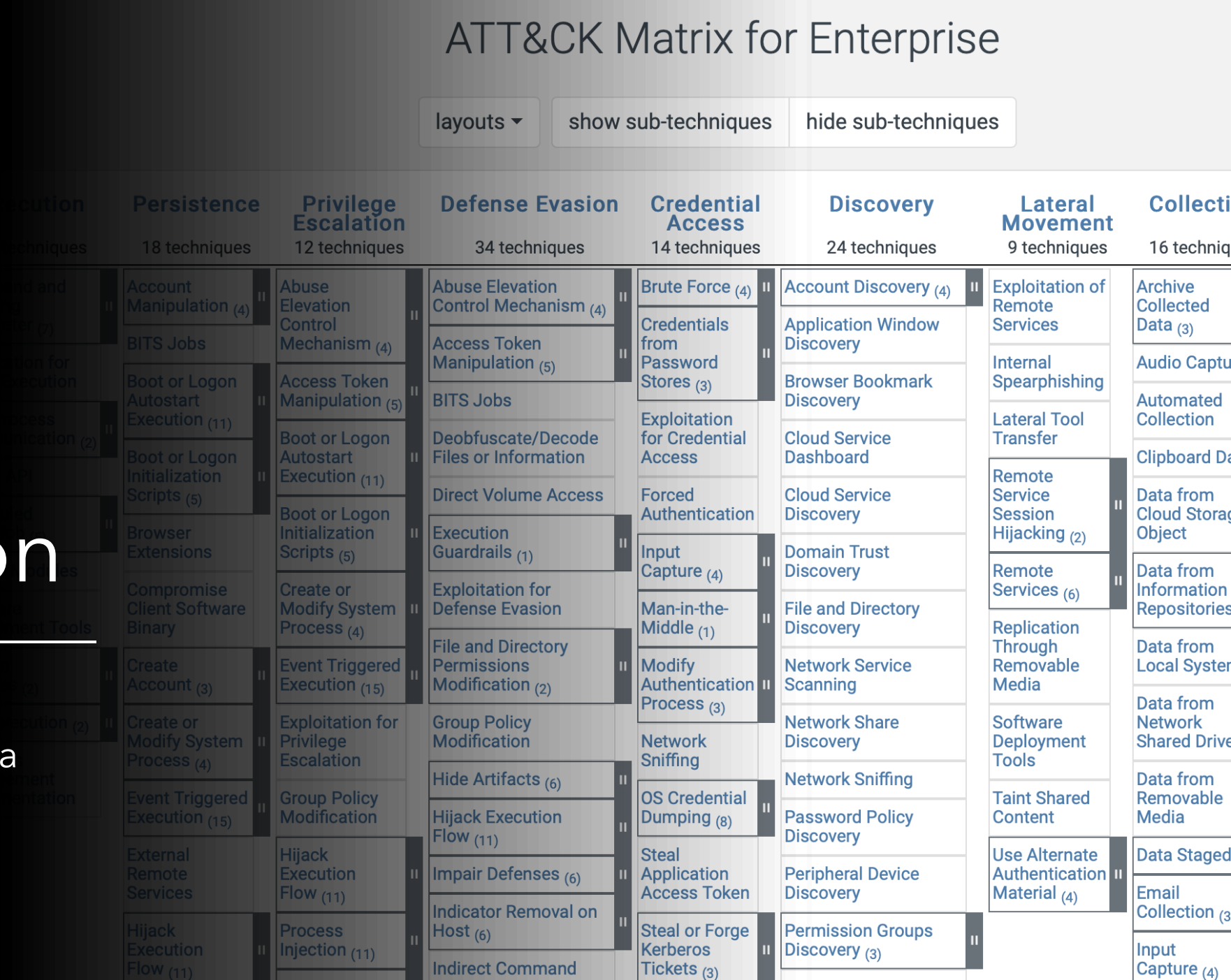

Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación
Resumir
Filtrar
Correlacionar
Visualizar


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

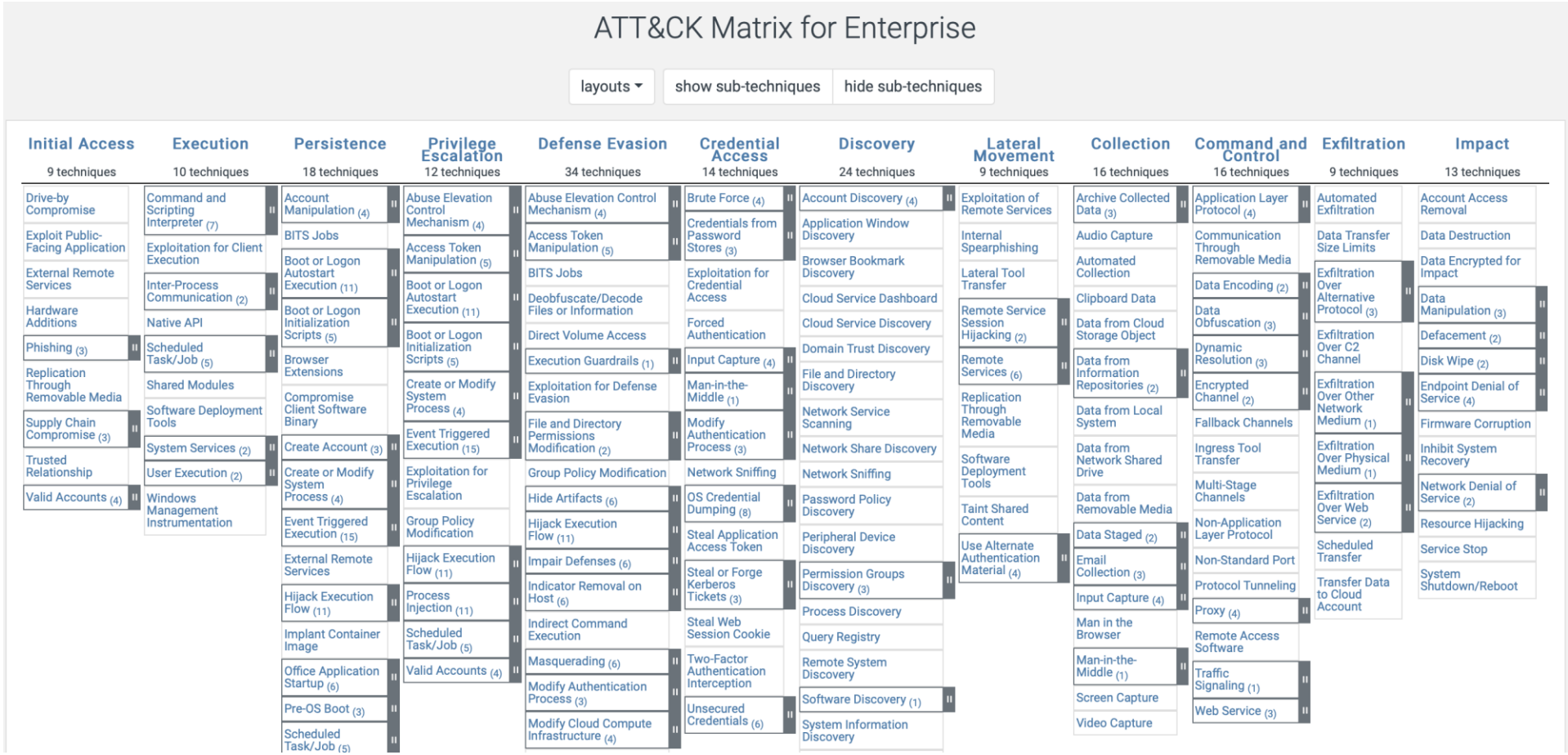

Generación de Set de Datos
Documentación de Eventos de Seguridad
Simulación del Adversario
Validación de Recolección de Datos

El Objetivo de la Investigación

Definiendo el alcance y tema para R&D

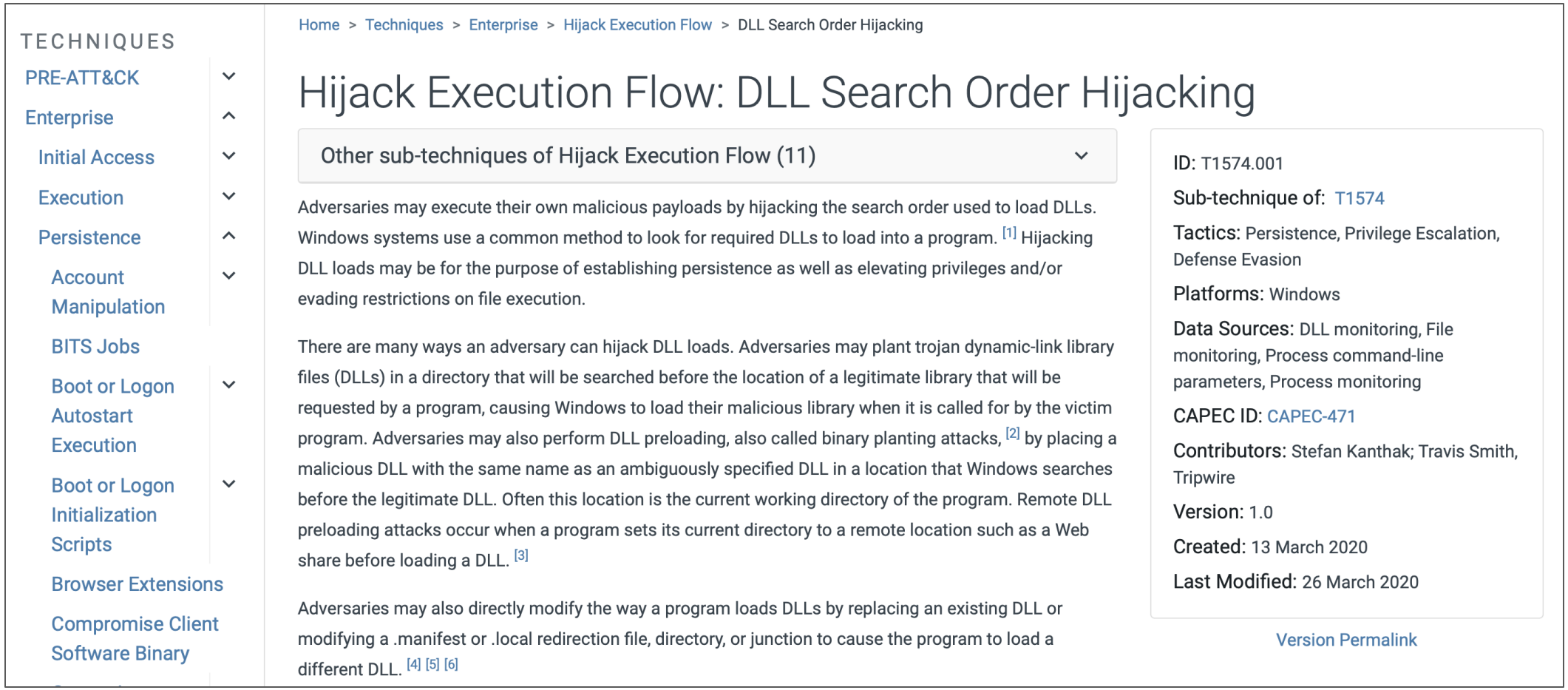


ATT&CK® framework



https://attack.mitre.org

ATT&CK® framework



TECHNIQUES

- PRE-ATT&CK
- Enterprise
  - Initial Access
  - Execution
  - Persistence
    - Account Manipulation
    - BITS Jobs
    - Boot or Logon Autostart Execution
    - Boot or Logon Initialization Scripts
    - Browser Extensions
    - Compromise Client Software Binary

Home > Techniques > Enterprise > Hijack Execution Flow > DLL Search Order Hijacking

Hijack Execution Flow: DLL Search Order Hijacking

Other sub-techniques of Hijack Execution Flow (11)

Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. [1] Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution.

There are many ways an adversary can hijack DLL loads. Adversaries may plant trojan dynamic-link library files (DLLs) in a directory that will be searched before the location of a legitimate library that will be requested by a program, causing Windows to load their malicious library when it is called for by the victim program. Adversaries may also perform DLL preloading, also called binary planting attacks, [2] by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. [3]

Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction to cause the program to load a different DLL. [4] [5] [6]

ID: T1574.001

Sub-technique of: T1574

Tactics: Persistence, Privilege Escalation, Defense Evasion

Platforms: Windows

Data Sources: DLL monitoring, File monitoring, Process command-line parameters, Process monitoring

CAPEC ID: CAPEC-471

Contributors: Stefan Kanthak; Travis Smith, Tripwire

Version: 1.0

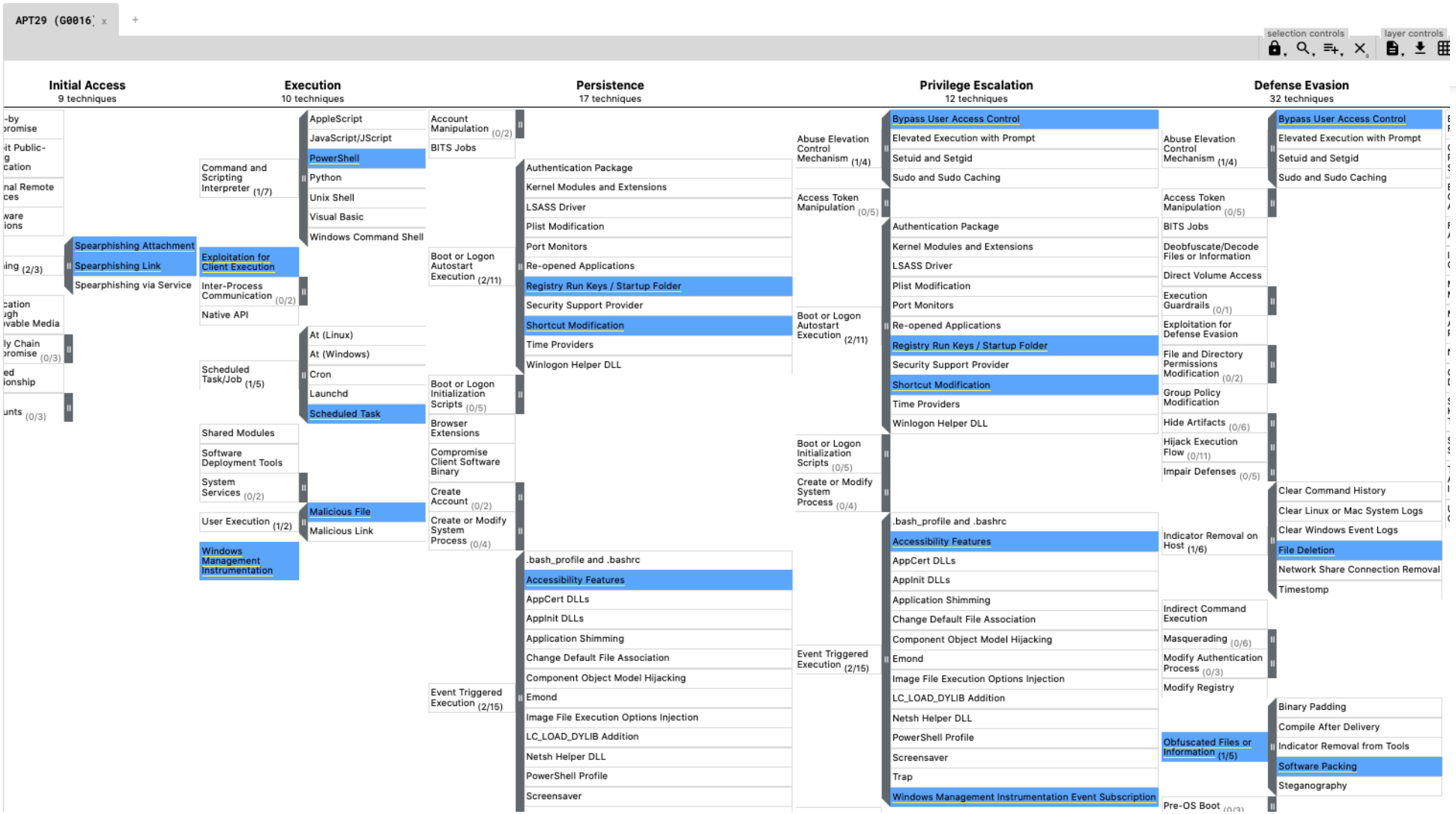
Created: 13 March 2020

Last Modified: 26 March 2020

Version Permalink

https://attack.mitre.org/techniques/T1574/001/

Evaluaciones via **ATT&CK®**

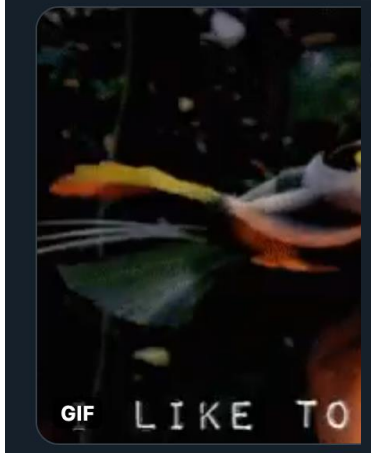


https://mitre-attack.github.io/attack-navigator/enterprise/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0016%2FG0016-enterprise-layer.json

Ingeligencia desde la comunidad

MDSec
@MDSecLabs

Part 1 in the "I Like to Move It" series on lateral movement by @domchell is now live... mdsec.co.uk/2020/09/i-like... #redtea



9:26 AM · Sep 1, 2020 · Twitte

120 Retweets **4** Quote Twe

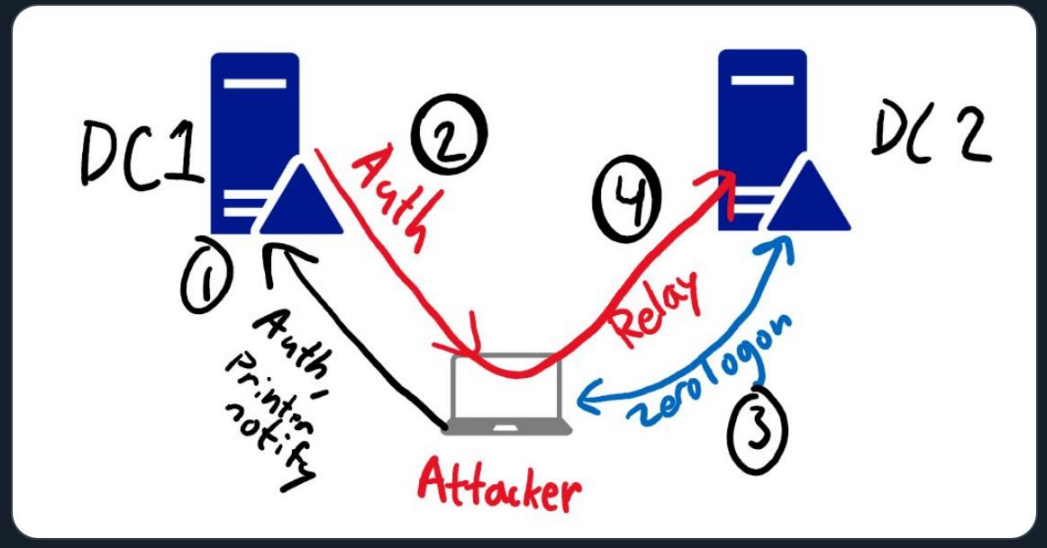
6

MDSec @MDSecLabs · Se
Part 2 in @domchell's serie
the blog mdsec.co.uk/202

1 103

Dirk-jan
@_dirkjan

New blog: A different way of abusing Zerologon. No more password reset needed: using the printer bug with Zerologon to relay to DRSUAPI and DCSync directly with ntlmrelayx: dirkjanm.io/a-different-wa...
Code: github.com/dirkjanm/CVE-2...



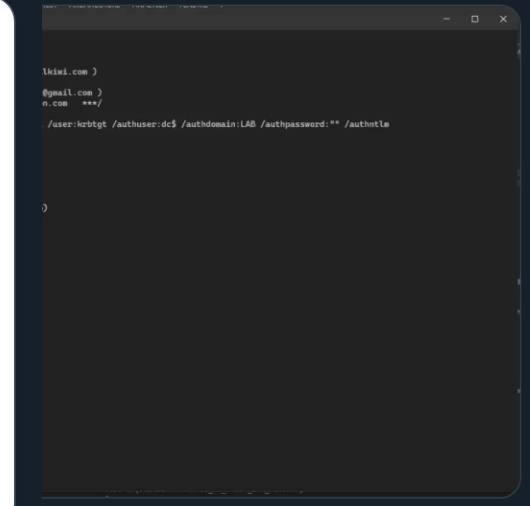
3:33 PM · Sep 24, 2020 · Twitter Web App

Benjamin Delpy

se with #zerologon / CVE-2020-1472
support and a lots of love inside ❤️

l (fast and supports unauthenticated on

m...

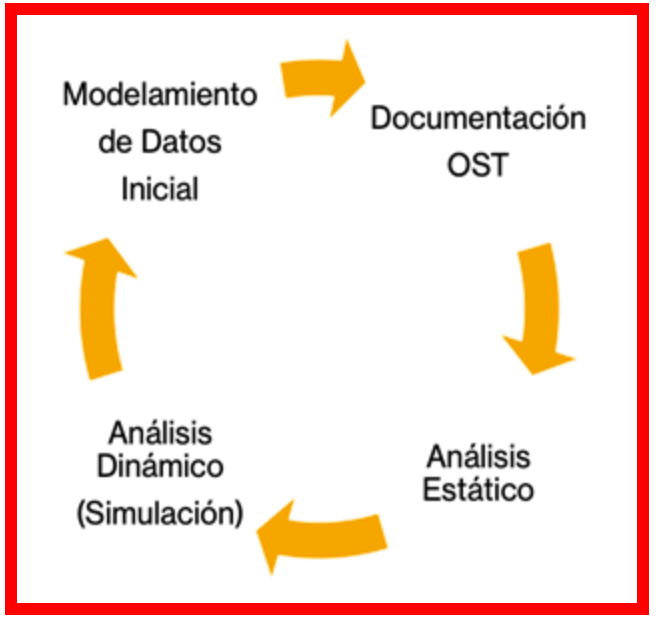


Web App

ets **1K** Likes


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)

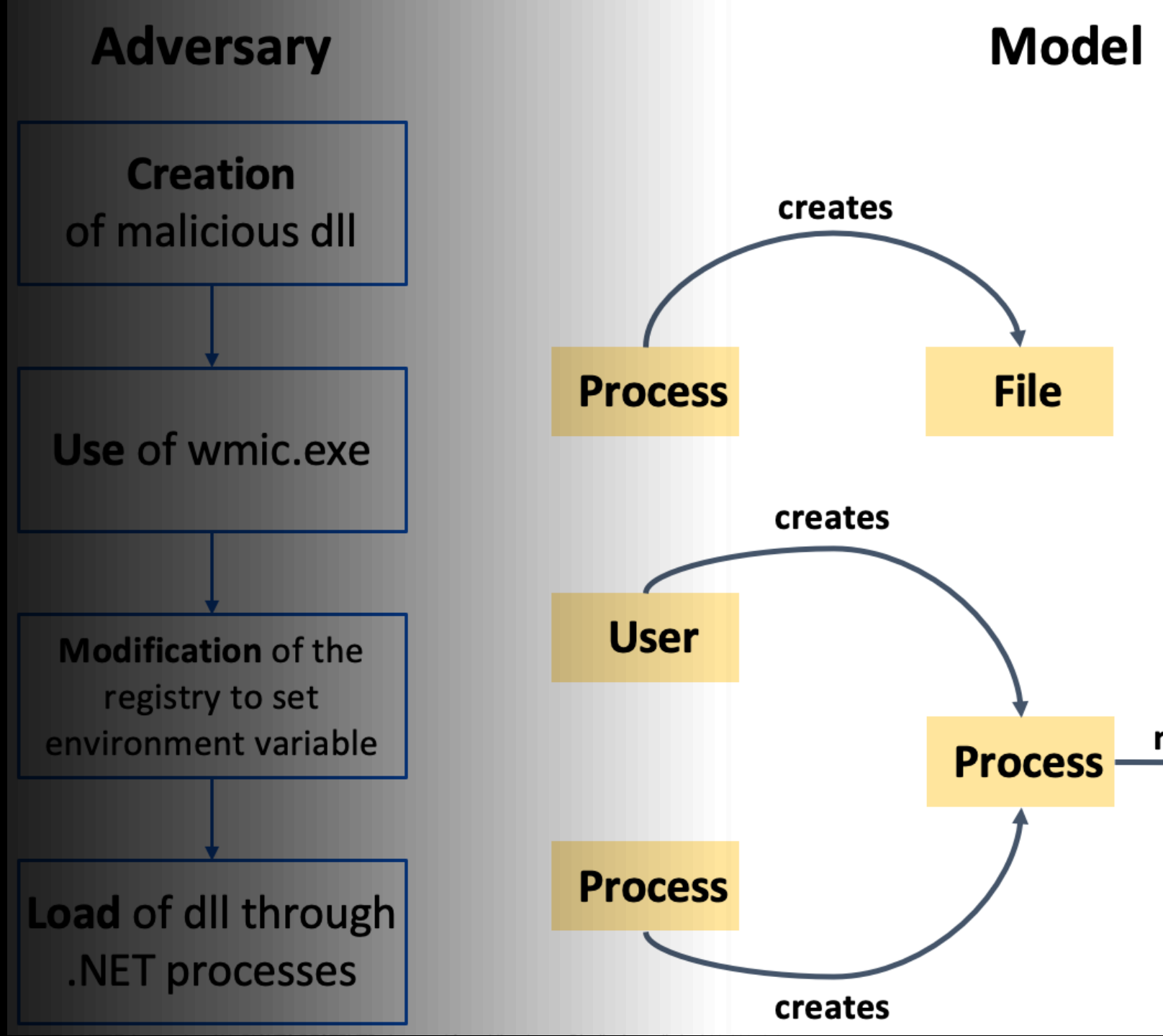

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Resumir
Filtrar
Correlacionar
Visualizar


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

Entendiendo al Adversario

La estrategia y el comportamiento



Movimiento Lateral con DCOM via ExecuteExcel4Macro

https://twitter.com/MDSecLabs/status/1306610061242925056

Aprendiendo el Comportamiento

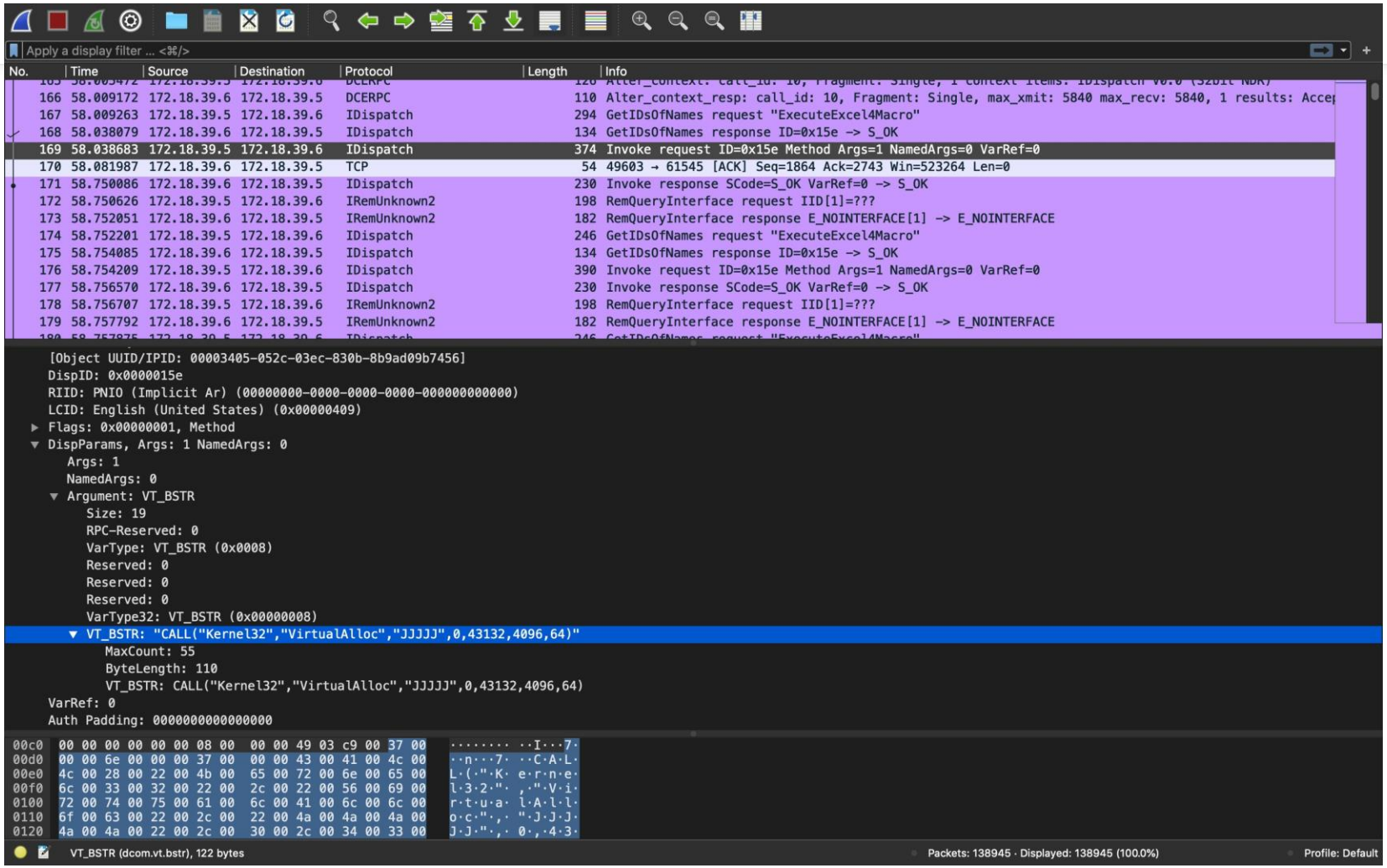
In order to weaponise this technique, we ideally want it to execute in a fileless manner. As explained by Outflank, XLM code has direct access to the Win32 API so we can leverage this to execute shellcode by writing it to memory and starting a new thread:

```
var memaddr = Convert.ToDouble(excel.GetType().InvokeMember("ExecuteExcel4Macro", BindingFlags.InvokeMet
var startaddr = memaddr;

foreach (var b in shellcode) {
        var cb = String.Format("CHAR({0})", b);
        var macrocode = "CALL(\\"Kernel32\\",\\"RtlMoveMemory\\",\\"JJCJ\\"," + memaddr + "," + cb + ",1
        excel.GetType().InvokeMember("ExecuteExcel4Macro", BindingFlags.InvokeMethod, null, excel, new o
        memaddr++;
}
excel.GetType().InvokeMember("ExecuteExcel4Macro", BindingFlags.InvokeMethod, null, excel, new object[]
```

This of course can be improved to do remote process injection or speed up execution by moving the bytes in chunks.

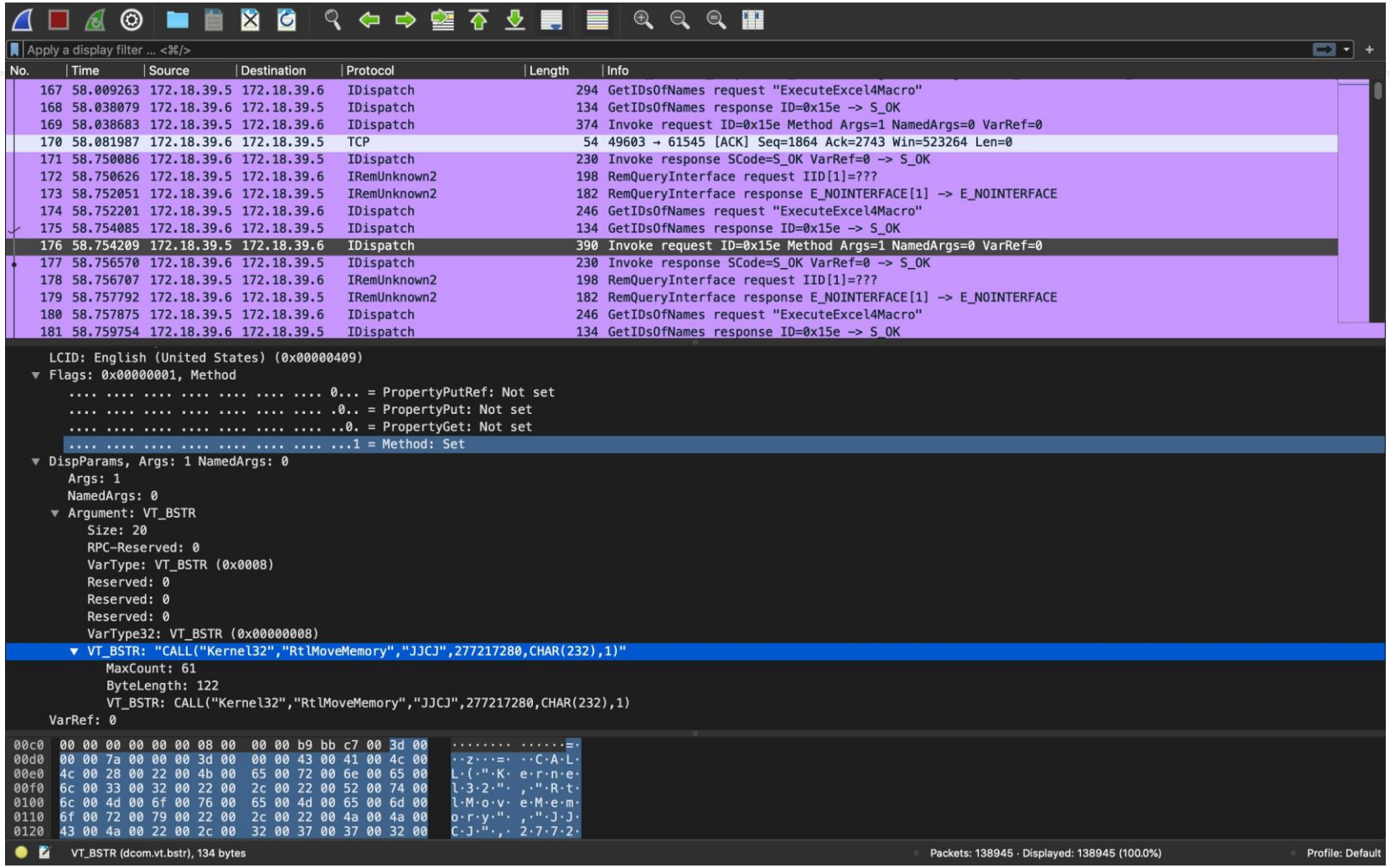
https://twitter.com/MDSecLabs/status/1306610061242925056

Análisis básico dinámico



https://twitter.com/MDSecLabs/status/1306610061242925056

Análisis básico dinámico



https://twitter.com/MDSecLabs/status/1306610061242925056

Entendiendo la estrategia del adversario

BlackSmith

https://github.com/OTRF/Blacksmith

SimuLand

https://github.com/OTRF/SimuLand

https://github.com/OTRF/mordor

BlackSmith

- Este proyecto se enfoca en proveer plantillas dinámicas y de fácil uso para investigadores de ciberseguridad con el objetivo de modelar y proveer recursos para la implementacion automatica de aplicaciones y ambientes de red en la nube.
- AWS CloudFormation & Microsoft Azure Resource Manager
- https://github.com/OTRF/Blacksmith

BlackSmith

master **Blacksmith** / templates / azure / Win10-DC / nestedtemplates / **customScriptExtension.json**

Cyb3rWard0g Sentinel2Go Draft Win10-DC ...

1 contributor

46 lines (46 sloc) | 1.41 KB

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "minLength": 1,
            "metadata": {
                "description": "Name of the windows machine to run scripts on"
            }
        },
        "extensionName": {
            "type": "string"
        },
        "fileUris": {
            "type": "array"
        },
        "commandToExecute": {
            "type": "string"
        },
        "location": {
            "type": "string",
```

master **Blacksmith** / templates / azure / Win10-DC / scripts / **Set-AD.ps1**

Cyb3rWard0g Updated Docs & Master compatible

1 contributor

15 lines (12 sloc) | 368 Bytes

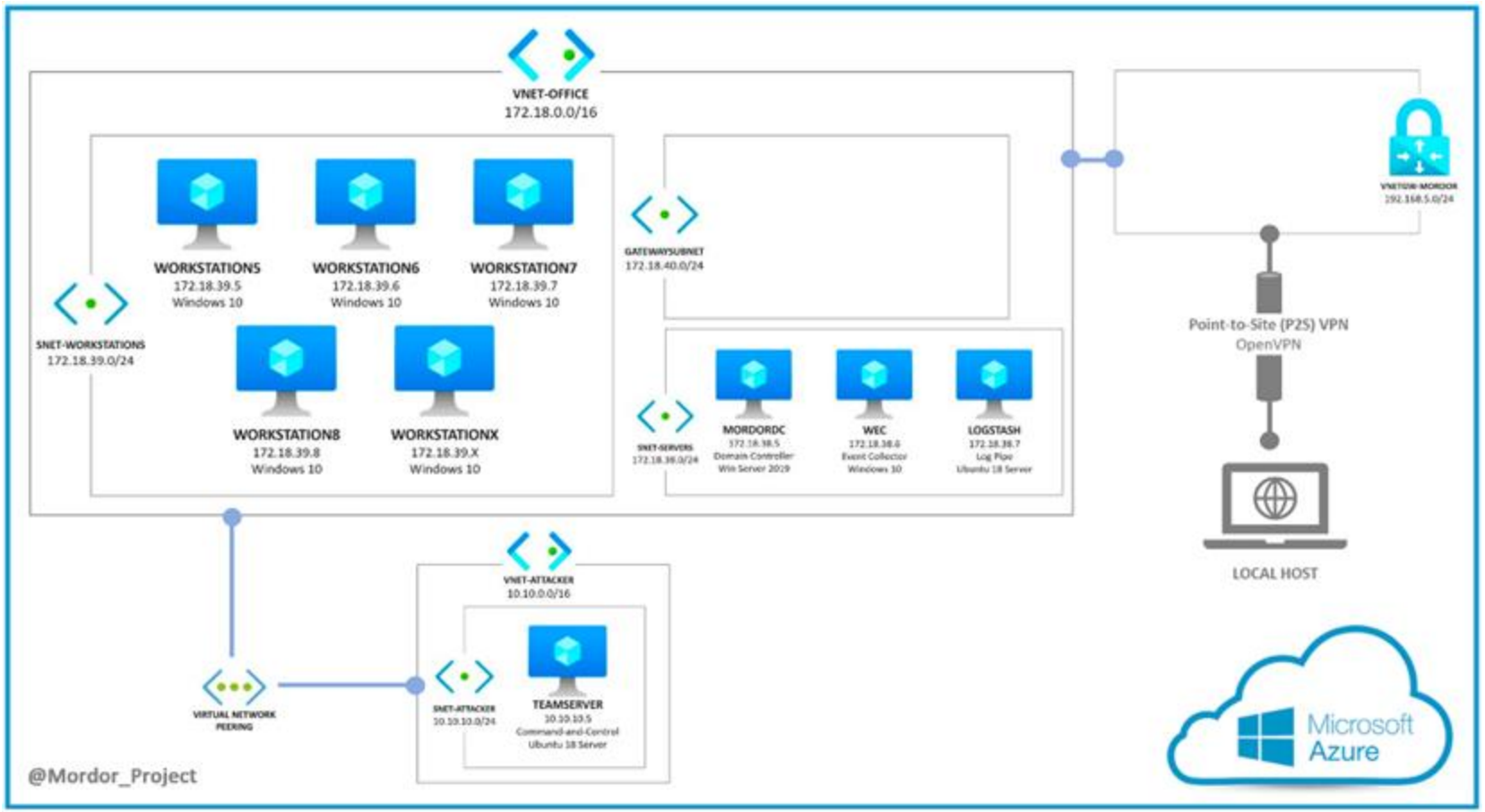
```
# Author: Roberto Rodriguez (@Cyb3rWard0g)
# License: GPL-3.0

[CmdletBinding()]
param(
    [Parameter(Mandatory=$true, Position=1)]
    [string]$domainFQDN,

    [Parameter(Mandatory=$true, Position=2)]
    [string]$dcVMName
)

& .\Set-OUs.ps1 -domainFQDN $domainFQDN
& .\Add-DomainUsers.ps1 -domainFQDN $domainFQDN -dcVMName $dcVMName
& .\Set-AuditSAMRemoteCalls.ps1
```

https://github.com/OTRF/Blacksmith

SimuLand

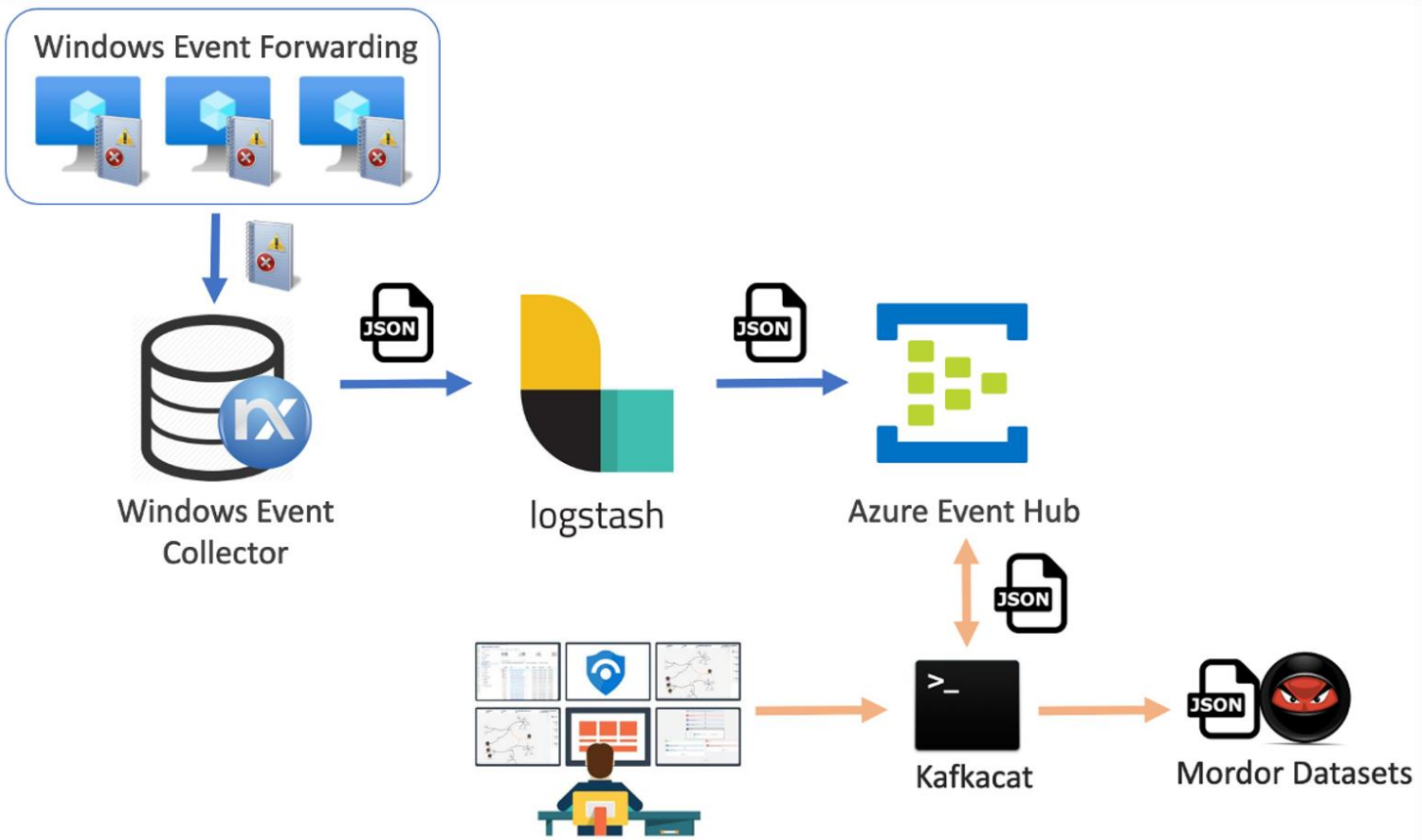
- C**loud templates** y **scripts:**
  - Simulación de adversarios
  - Generación-recolección de datos
  - Enfocado en el aprendizaje de la estrategia del adversario desde una perspectiva de datos.
- M**últiples ambientes modulares** que permiten la adaptación de requerimientos específicos de un tema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

The Shire (Windows)



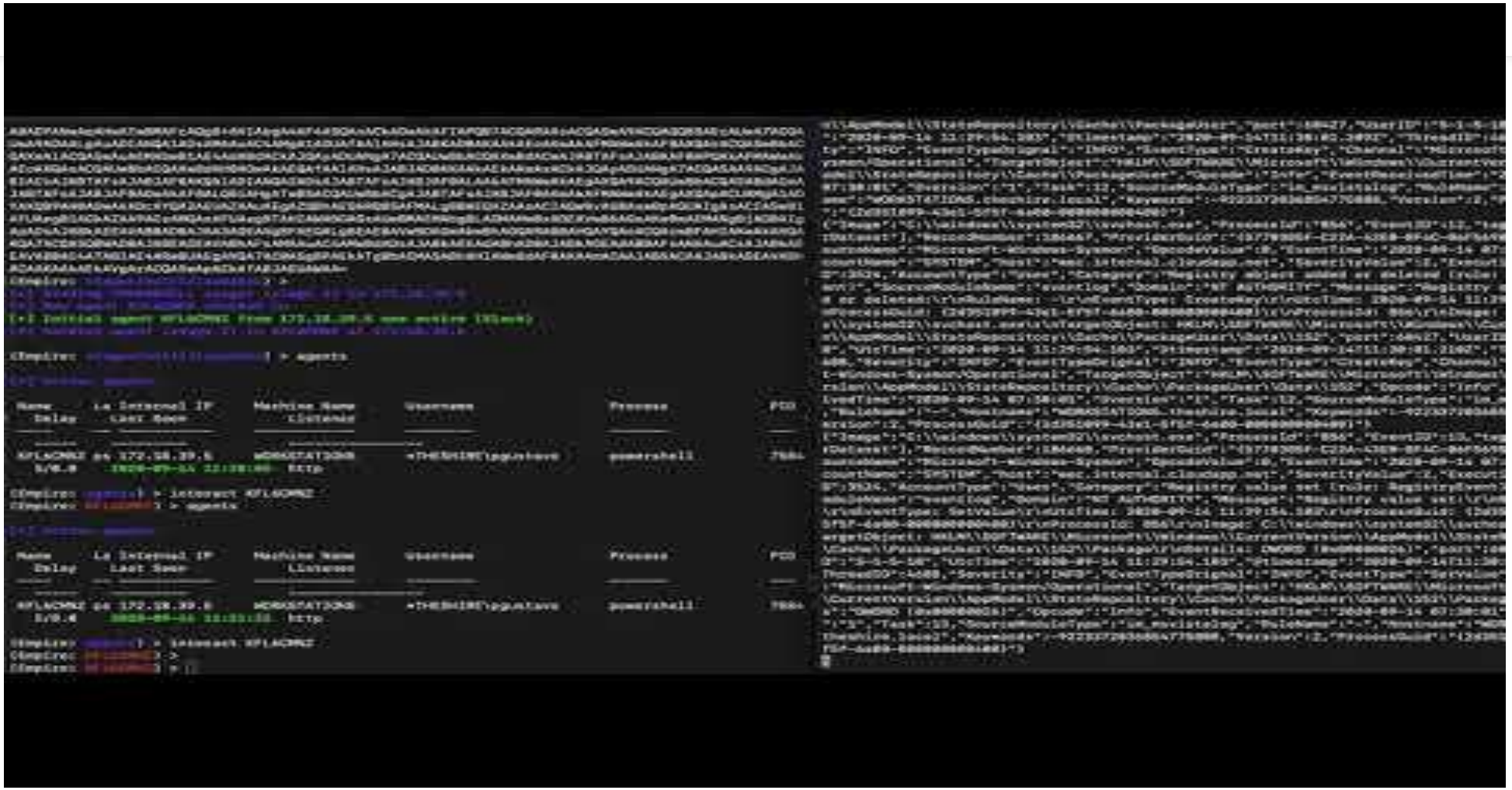
https://github.com/OTRF/SimuLand/tree/master/environments/windows/shire

The Shire (Windows)



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

Simula -> Exporta



https://youtu.be/x4STX5RlNJo

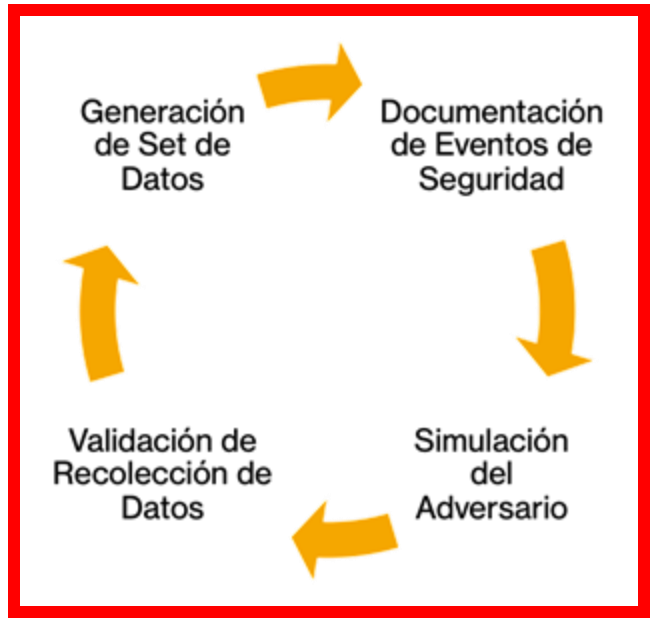

SIEM agnóstico
Modular & Integrado
Interactivo & Replicable
Impulsado por la comunidad


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

Recolectando y documentando data

Generando data en Casa

Actividades Básicas al simular al adversario

Planificación

Emulacion

Habilitar telemetría

Recolectar y analizar datos

Puedo detectarlo?

No

Si

Documentar Resultados

Cómo? Dónde? Cuándo?

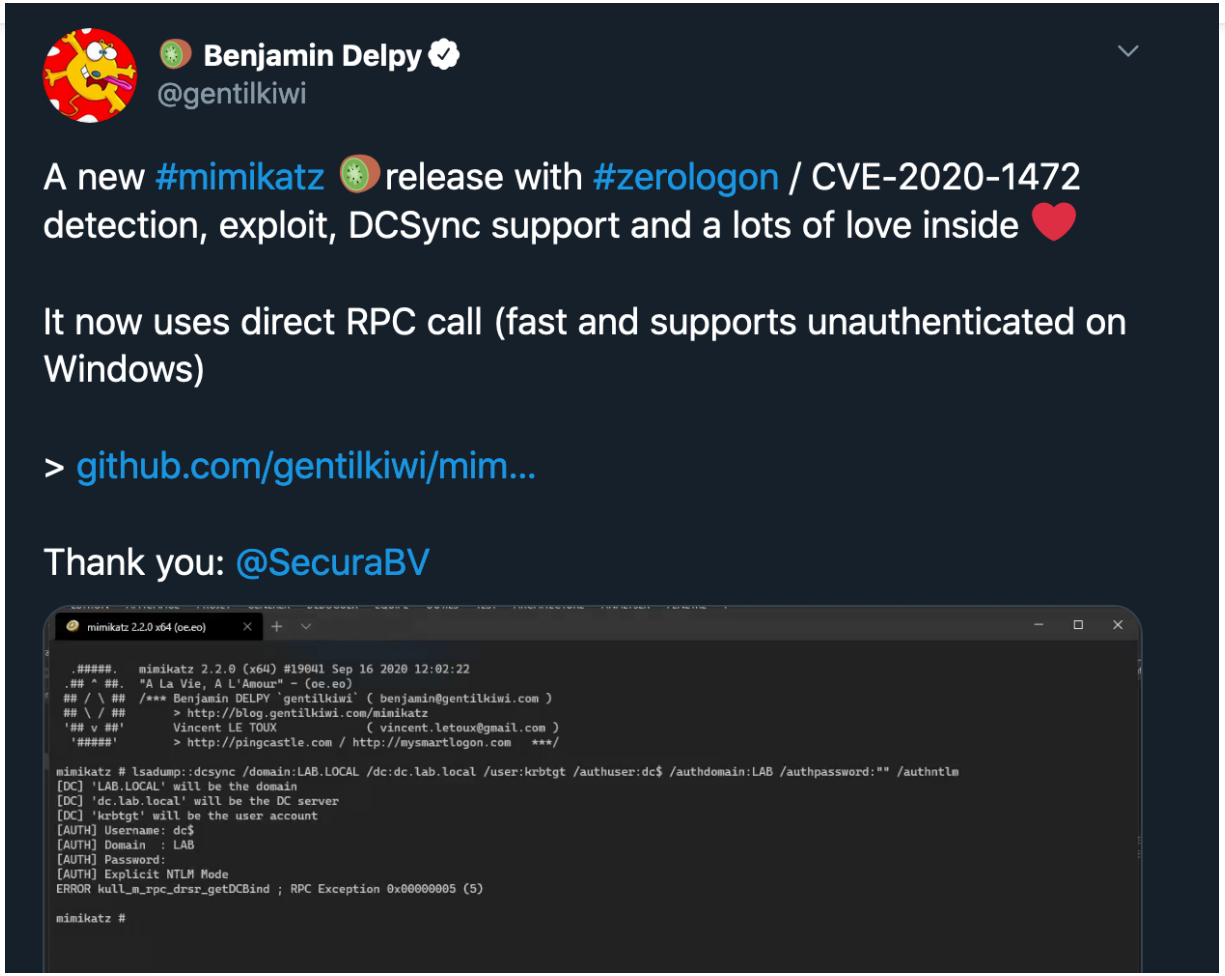
Planificación	Emulación
	
Recolectar y Analizar	**Habilitar Telemetría**
	

Documentar resultados


Desafíos

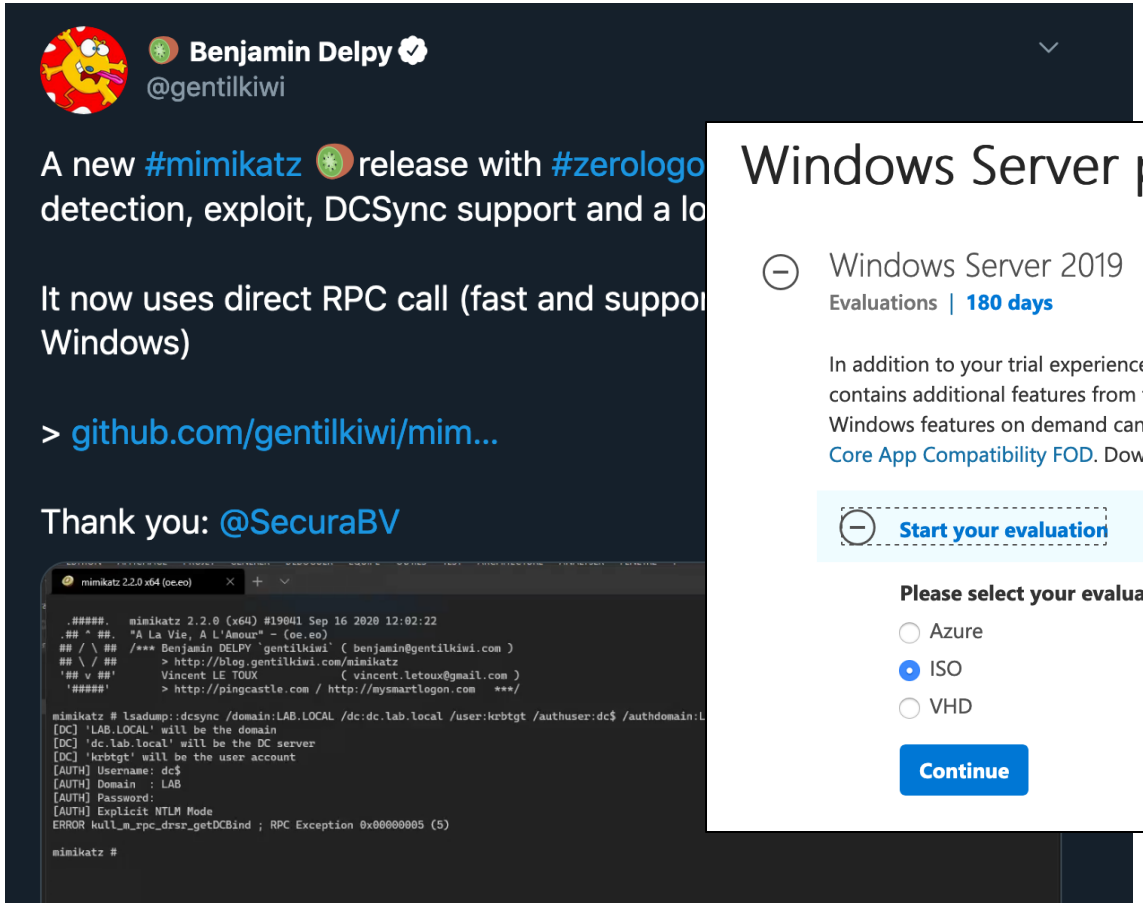
- Puede requerir alta inversión de **tiempo** y **tecnología**
- Pueda que tengas que escribir tus propias herramientas
- Configurar la colección de datos es más que un solo comando o switch

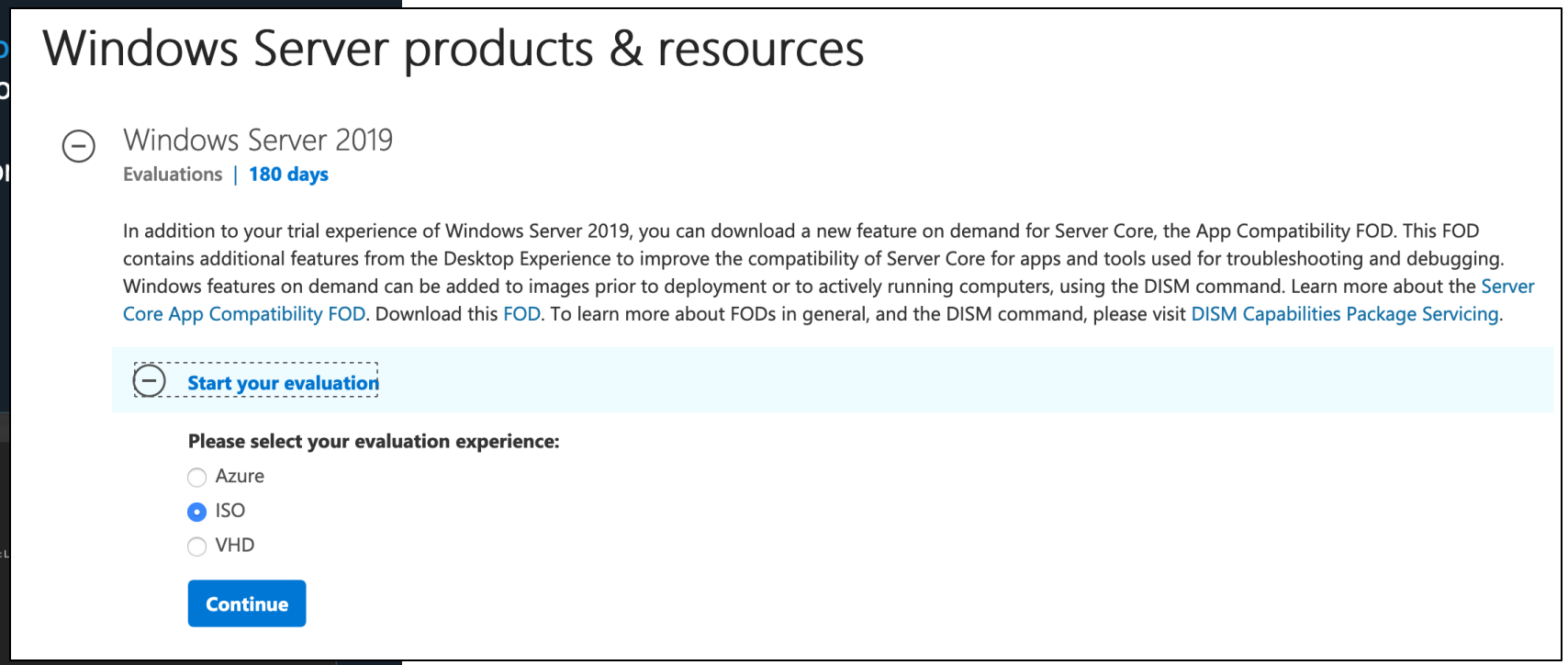
Ejemplos? Por que es complicado?



https://twitter.com/gentilkiwi/status/1306178689630076929

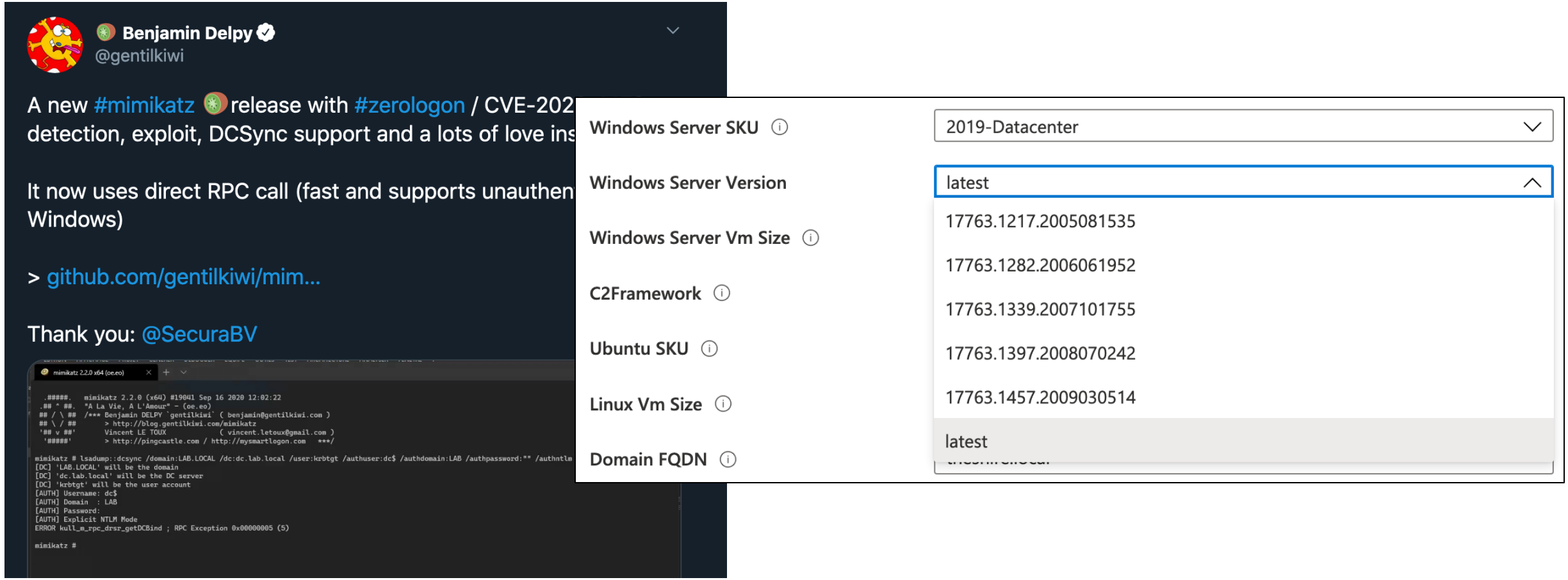
Ejemplos? Por que es complicado?





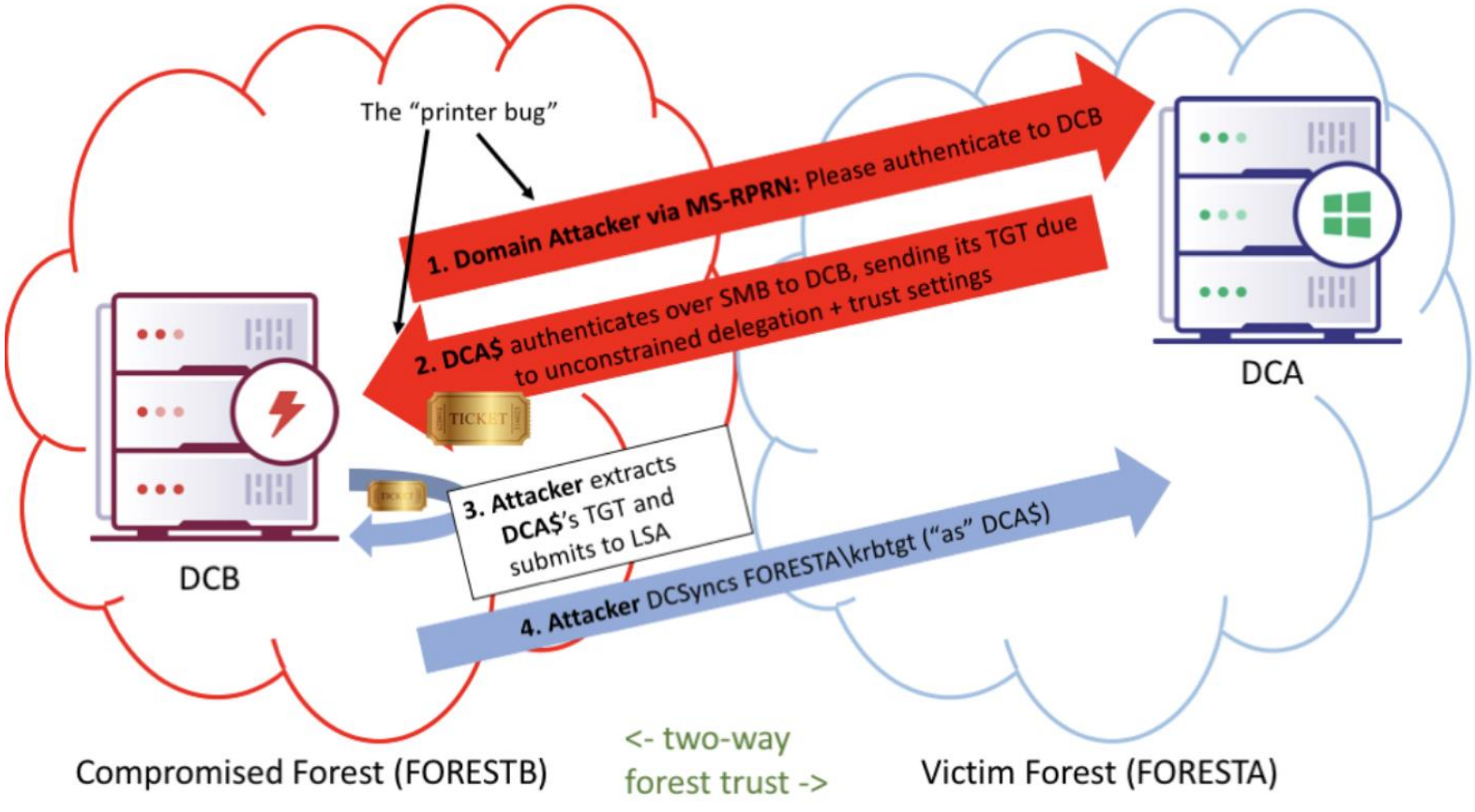
https://twitter.com/gentilkiwi/status/1306178689630076929

Ejemplos? Por que es complicado?



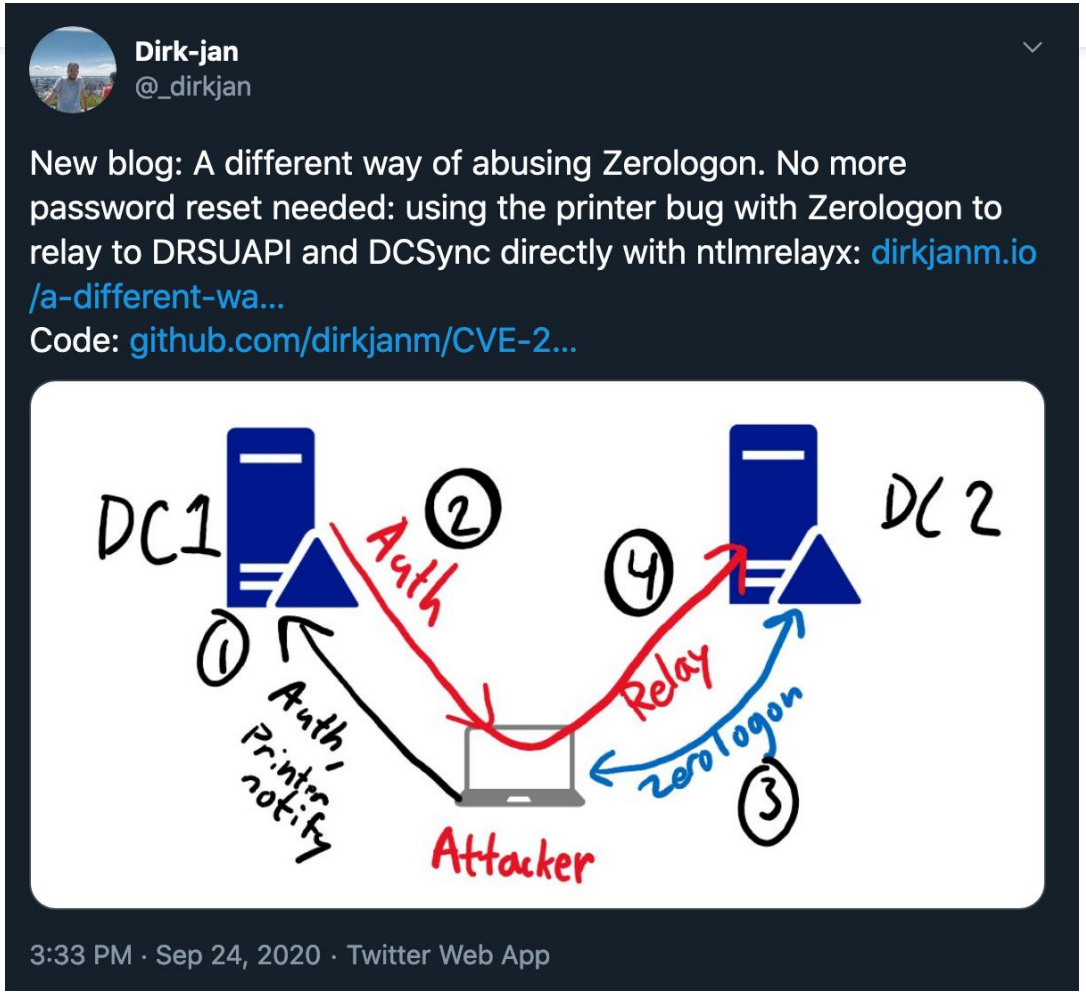
https://twitter.com/gentilkiwi/status/1306178689630076929

Ejemplos? Por que es complicado?



https://www.harmj0y.net/blog/redteaming/not-a-security-boundary-breaking-forest-trusts/

Ejemplos? Por que es complicado?

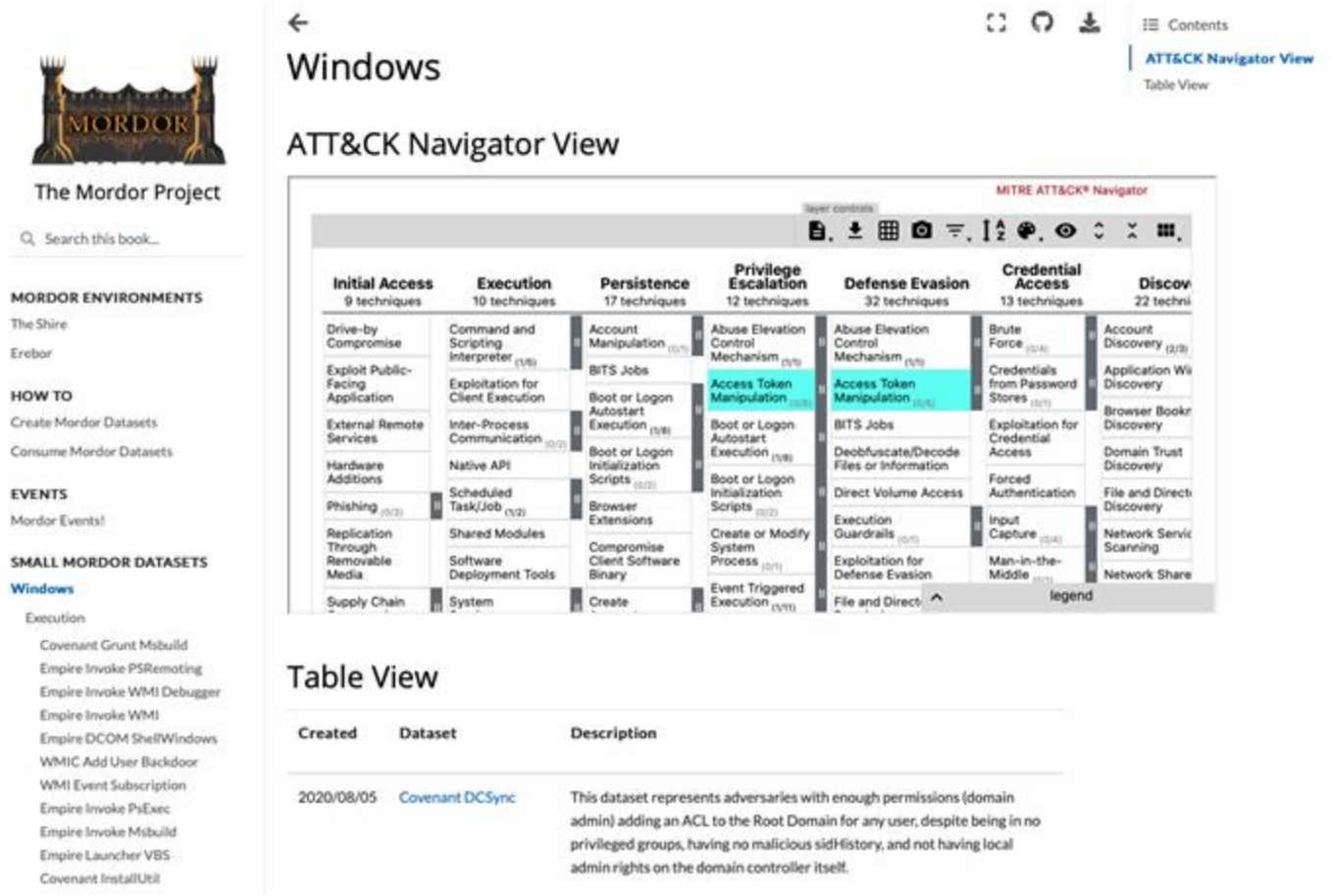


https://twitter.com/_dirkjan/status/1309214379003588608

@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



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

Mordor: Septiembre 25 @15:30-16:30

Qué podemos hacer con la data?

Mordor Files

- Entrenamiento de analistas de seguridad
- Entrevistas de trabajo
- Eventos (Hackathons)
- Validación de analiticos desarrollados in-house

OSSEM (Open Source Security Event Metadata)

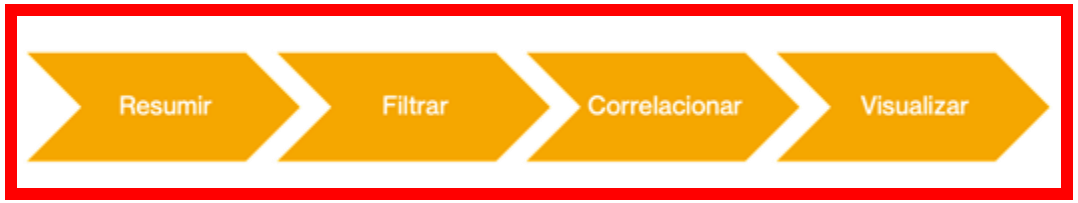
- Diccionarios de Datos
  - Windows (Security, Sysmon)
- Modelos de Datos
  - Elementos de datos
  - Relaciones
- Modeo de Informacion Común
  - Standarización


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)

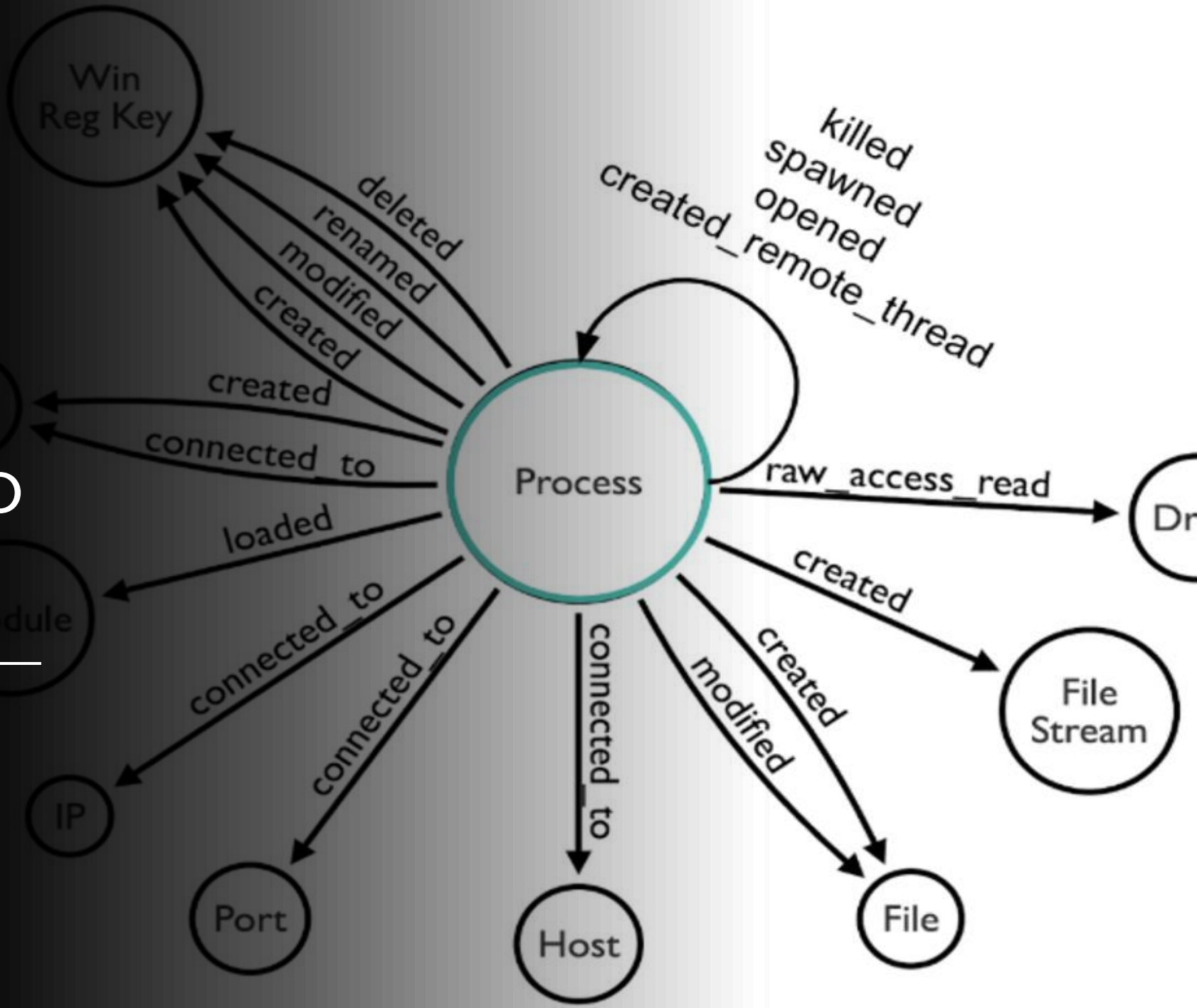

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Resumir
Filtrar
Correlacionar
Visualizar


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

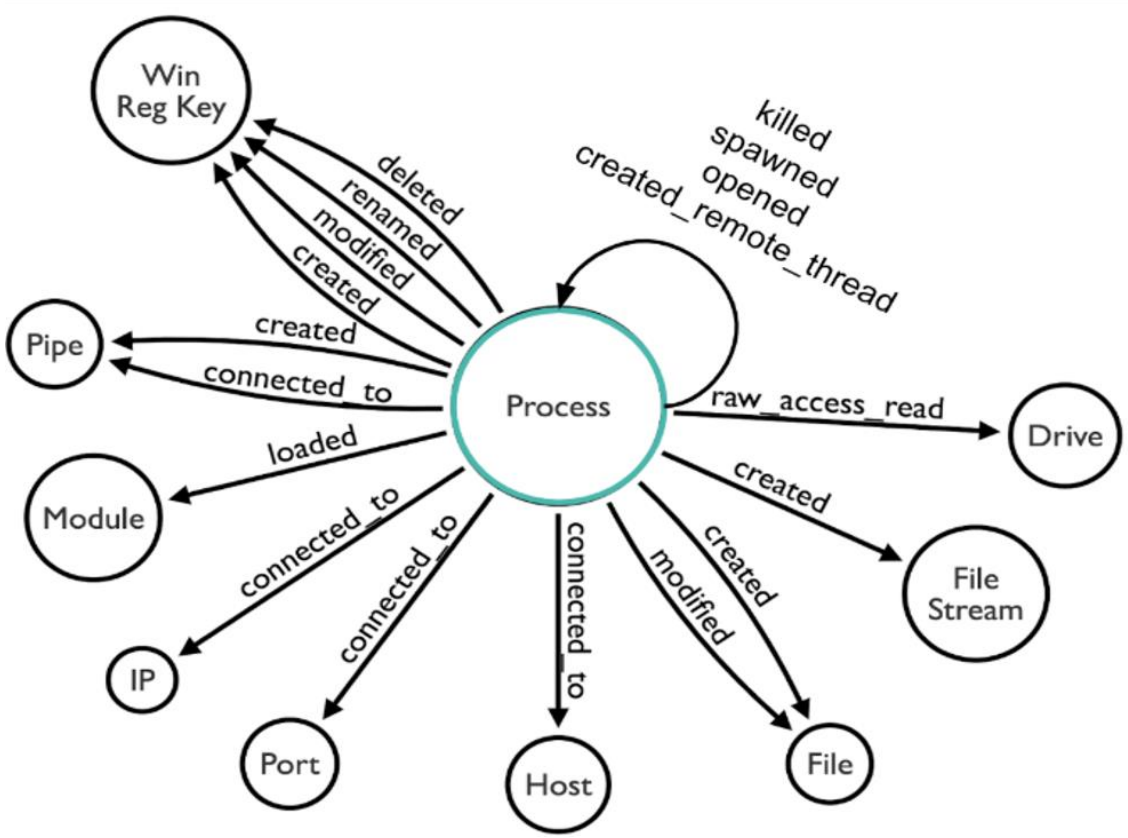
Análisis y Modelamiento de Datos

Representando al Adversario



Modelamiento de Datos

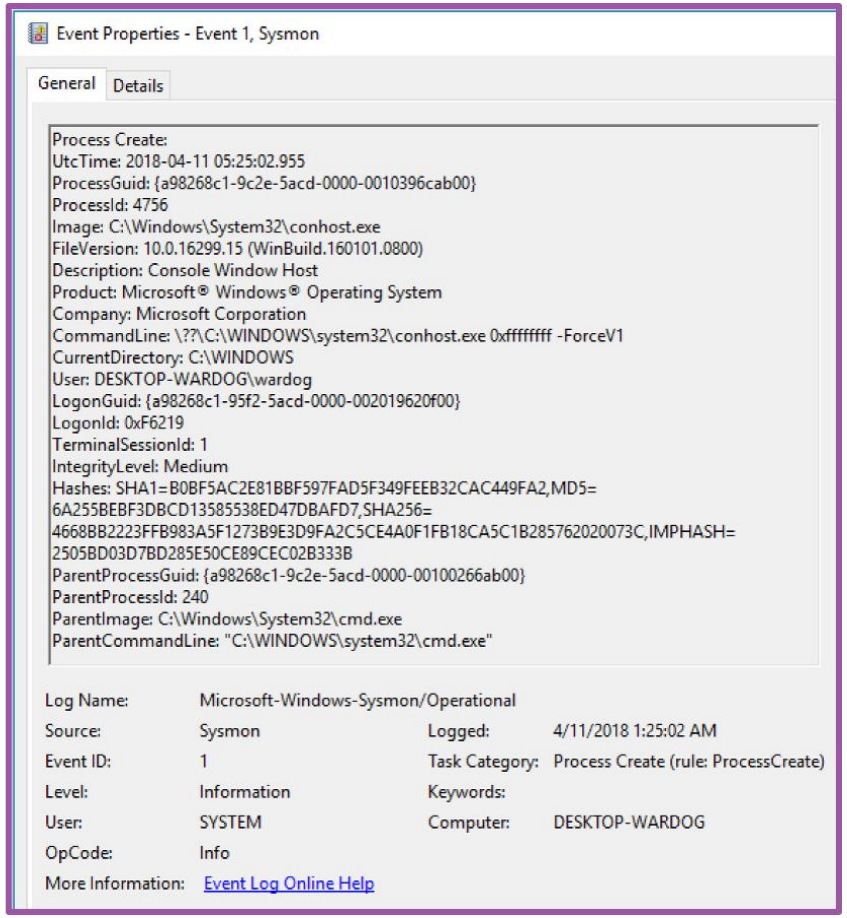
Un modelo de datos nos permite **organizar elementos de datos** que consideramos relevantes para nuestro análisis y estandarizar **la relación que existen entre ellos**



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

¿Cómo identificar elementos de datos y relaciones?

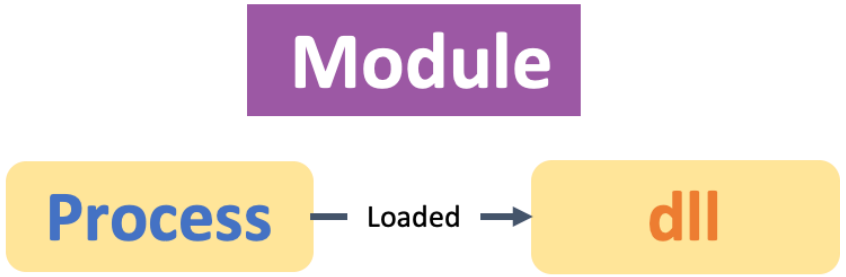
Un **diccionario de datos** describe un evento de seguridad y los atributos de datos que lo describen



Documentando eventos de seguridad

Sysmon 7
Image Loaded

Field	Type	Description	Sample Value
Process Guid	String	Process Guid of the process that loaded the image	{A98268C1-A12A-5ACD-0000-0010E4C8B300}
Process Id	Integer	Process ID used by the os to identify the process that loaded the image	3532
Image	String	File path of the process that loaded the image	C:\Windows\System32\cmd.exe
Image Loaded	String	Full path of the image loaded	C:\Windows\System32\msvcrt.dll
Description	String	Description of the image loaded	Windows NT CRT DLL



Ejemplo: Modelando el uso de **COR_PROFILER**

Home > Techniques > Enterprise > Hijack Execution Flow > COR_PROFILER

Hijack Execution Flow: COR_PROFILER

Other sub-techniques of Hijack Execution Flow (11)

Adversaries may leverage the COR_PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded into each .NET process that loads the Common Language Runtime (CLR). These profiliers are designed to monitor, troubleshoot, and debug managed code executed by the .NET CLR.[1][2]

The COR_PROFILER environment variable can be set at various scopes (system, user, or process) resulting in different levels of influence. System and user-wide environment variable scopes are specified in the Registry, where a Component Object Model (COM) object can be registered as a profiler DLL. A process scope COR_PROFILER can also be created in-memory without modifying the Registry. Starting with .NET Framework 4, the profiling DLL does not need to be registered as long as the location of the DLL is specified in the COR_PROFILER_PATH environment variable.[2]

Adversaries may abuse COR_PROFILER to establish persistence that executes a malicious DLL in the context of all .NET processes every time the CLR is invoked. The COR_PROFILER can also be used to elevate privileges (ex: Bypass User Access Control) if the victim .NET process executes at a higher permission level, as well as to hook and Impair Defenses provided by .NET processes.[3][4][5][6][7]

ID: T1574.012

Sub-technique of: T1574

Tactics: Persistence, Privilege Escalation, Defense Evasion

Platforms: Windows

Permissions Required: Administrator, User

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

Contributors: Jesse Brown, Red Canary

Version: 1.0

Created: 24 June 2020

Last Modified: 26 June 2020

Version Permalink

https://attack.mitre.org/techniques/T1574/012/

Ejemplo: Modelando el uso de **COR_PROFILER**

Adversario habilita **COR_ENABLE_PROFILING** variable

Adversario configura el CLSID de la variable **COR_PROFILER,** el cual identifica la ubicacion de la DLL

Adversario registra la DLL usando la **InProcServer32** sunkey en el registry y asociandola al mismo CLSID

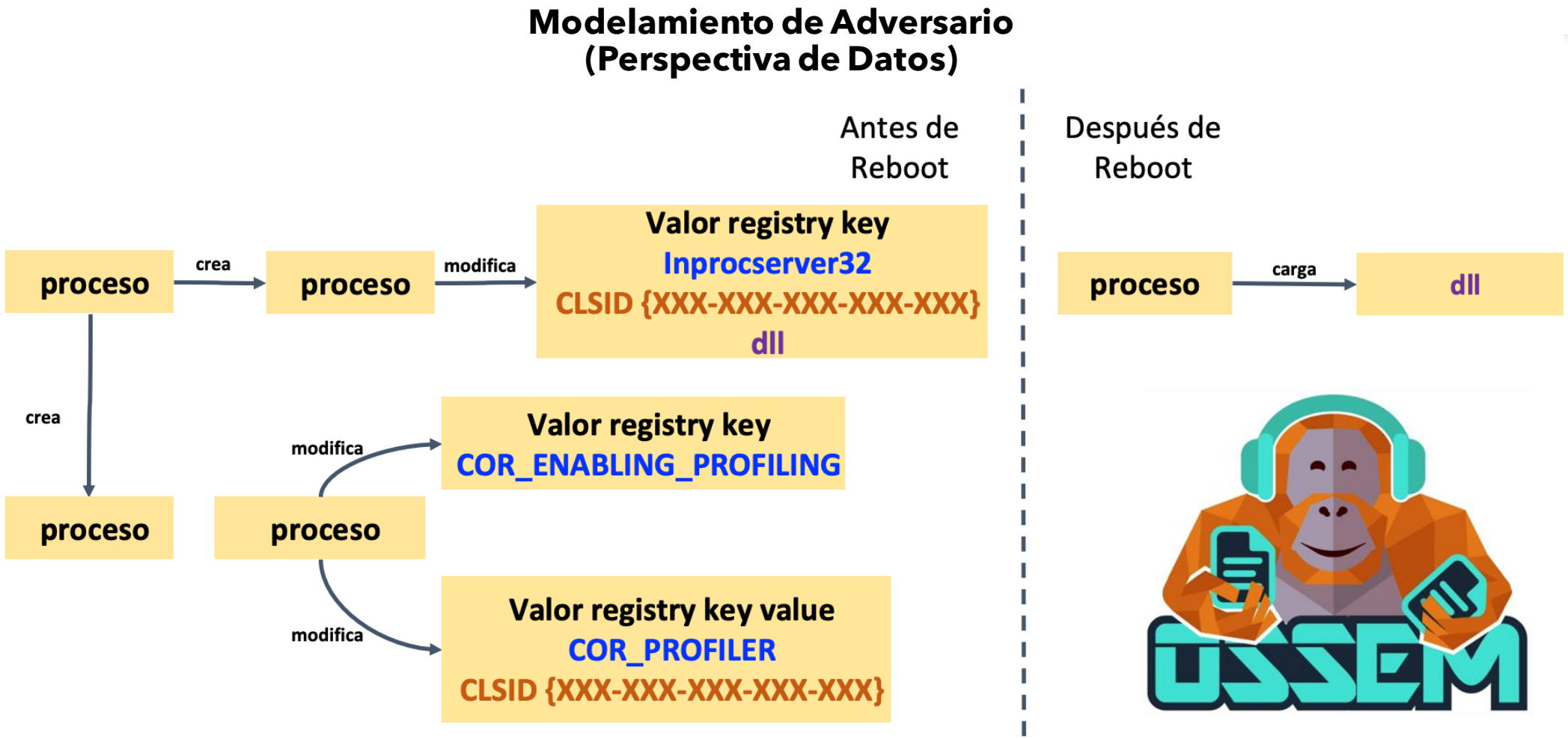
```
wmic ENVIRONMENT create
name="COR_ENABLE_PROFILING",username="",VariableValue="1"
```

```
wmic ENVIRONMENT create
name="COR_PROFILER",username="",VariableValue=""

REG.EXE ADD HKEY_LOCAL_MACHINE\Software\Classes\CLSID\\InProcServer32
/V ThreadingModel /T REG_SZ /D Apartment /F
```

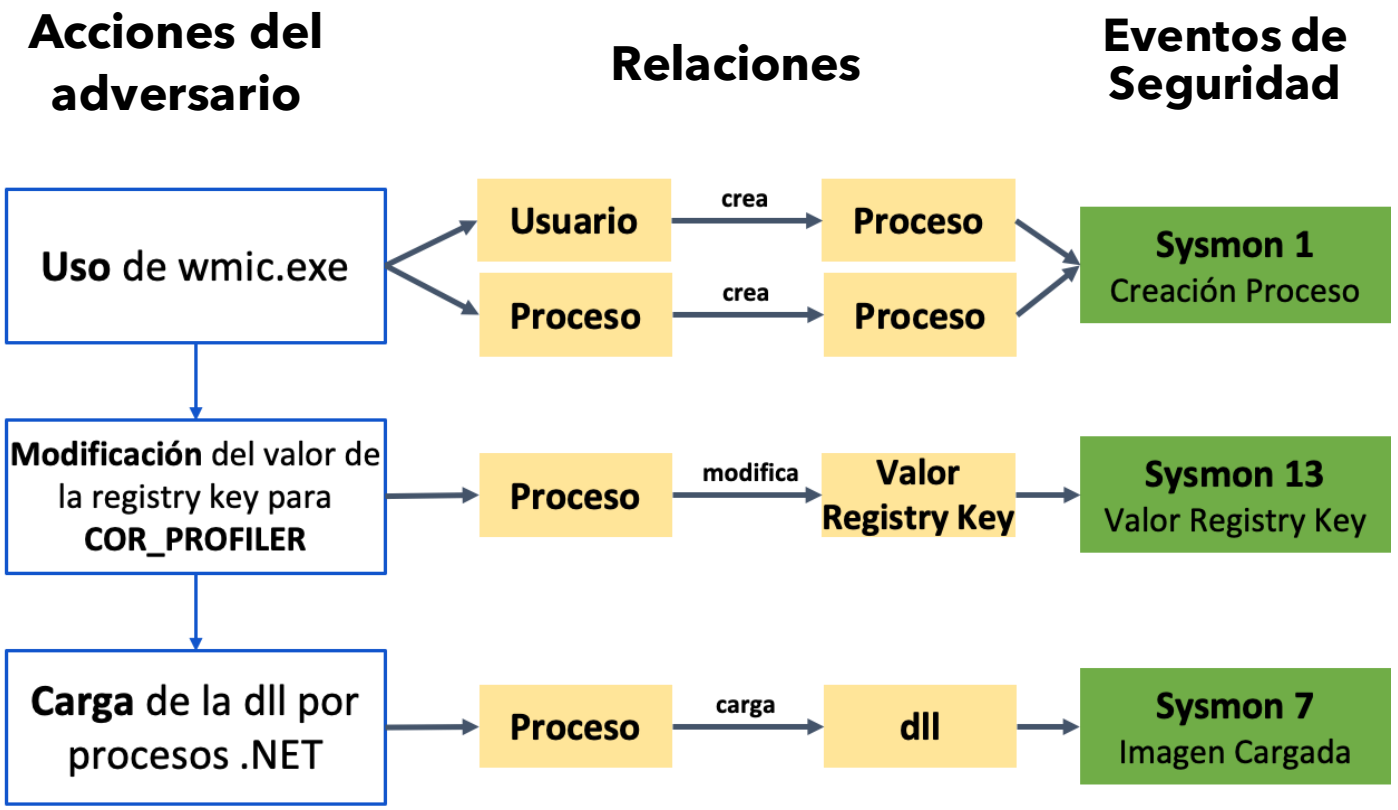
```
REG.EXE ADD HKEY_LOCAL_MACHINE\Software\Classes\CLSID\\InProcServer32
/VE /T REG_SZ /D "c:\windows\System32\e0b3489da74f.dll" /F
```

https://redcanary.com/blog/cor_profiler-for-persistence/

Ejemplo: Modelando el uso de **COR_PROFILER**



Ejemplo: Modelando el uso de **COR_PROFILER**



Jupyter Notebooks

- Limpieza y transformación de data
- Visualización de data
- Modelamiento estadístico de datos
- Aplicaciones de machine learning y mas..

https://jupyter.org/

¿Qué son Jupyter Notebooks?

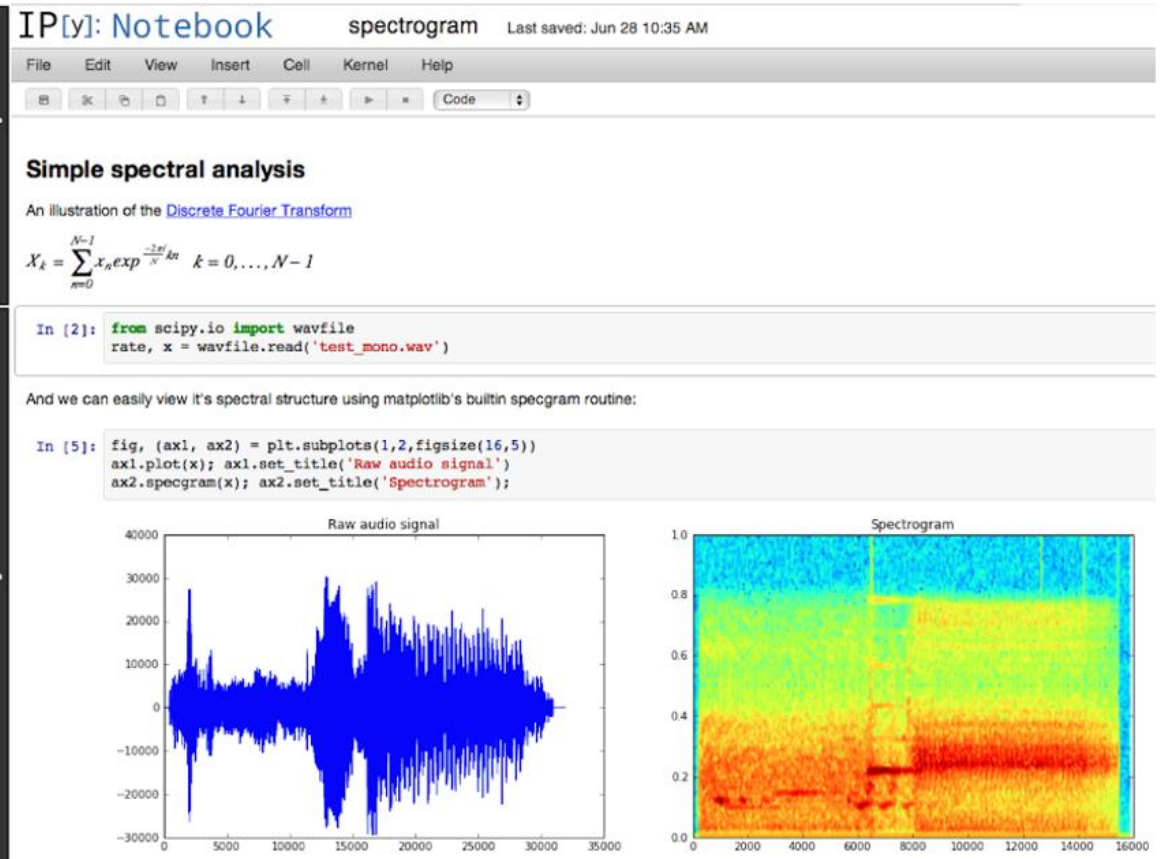
- Son documentos que podemos accesar a través de una interface web. Nos permite gestionar y almacenar:
  - **Input:** Código (por ejemplo Python)
  - **Output**: Resultados de Código ejecutado
- Excelente para contar la historia de la investigacion desarrollada.

https://jupyter.org/

Python Interpreter -> IPython -> Jupyter

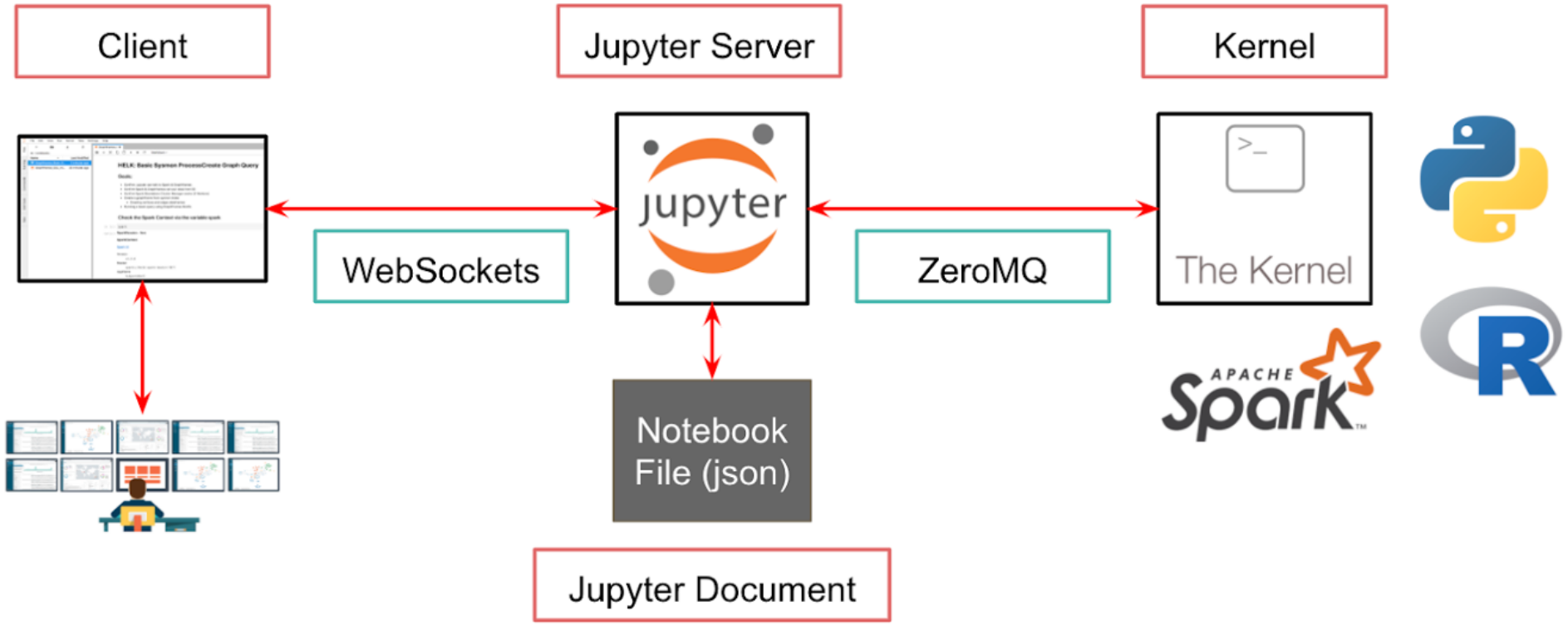
```
Robertos-MacBook-Pro:~ wardog$ python3
Python 3.7.2 (default, Feb 12 2019, 08:16:38)
[Clang 10.0.0 (clang-1000.11.45.5)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> print('Hola Python!!')
Hola Python!!
>>> 12 * 2
24
>>>
```

```
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]:
```



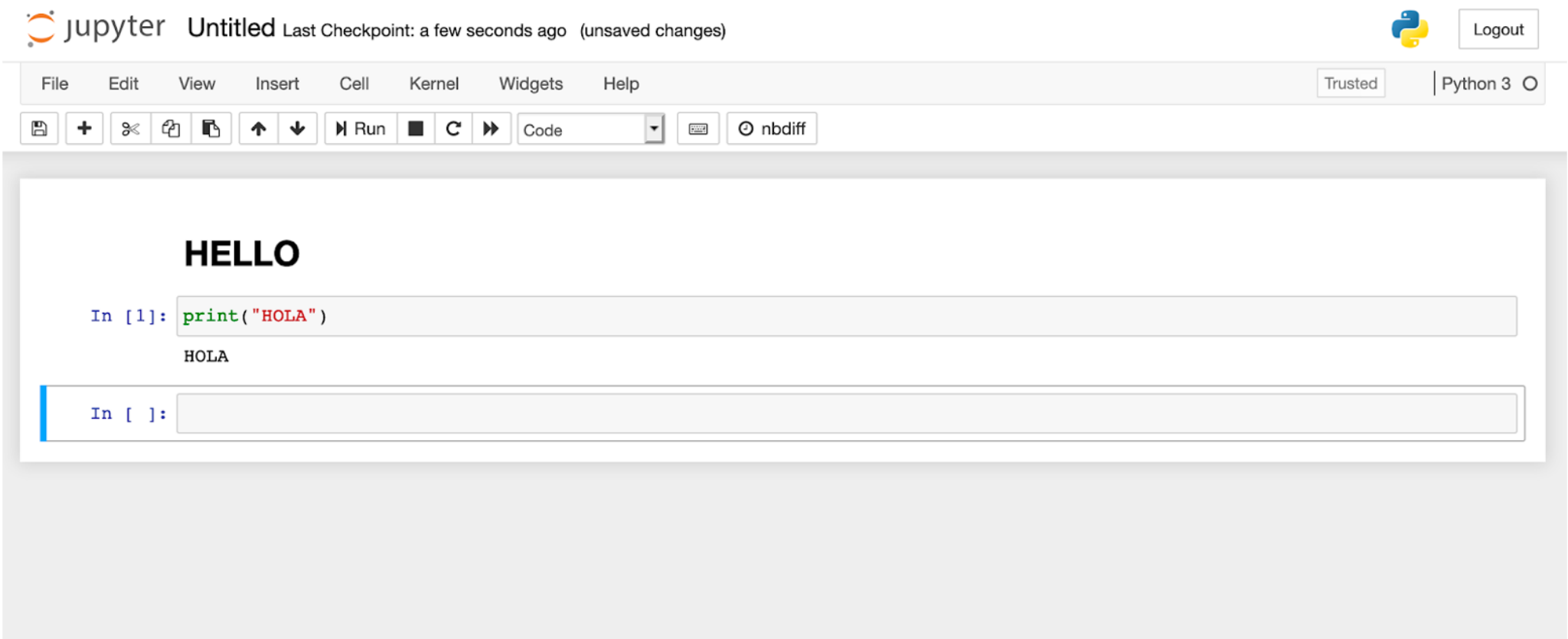
https://jupyter.org/

La arquitectura básica de Jupyter Notebooks



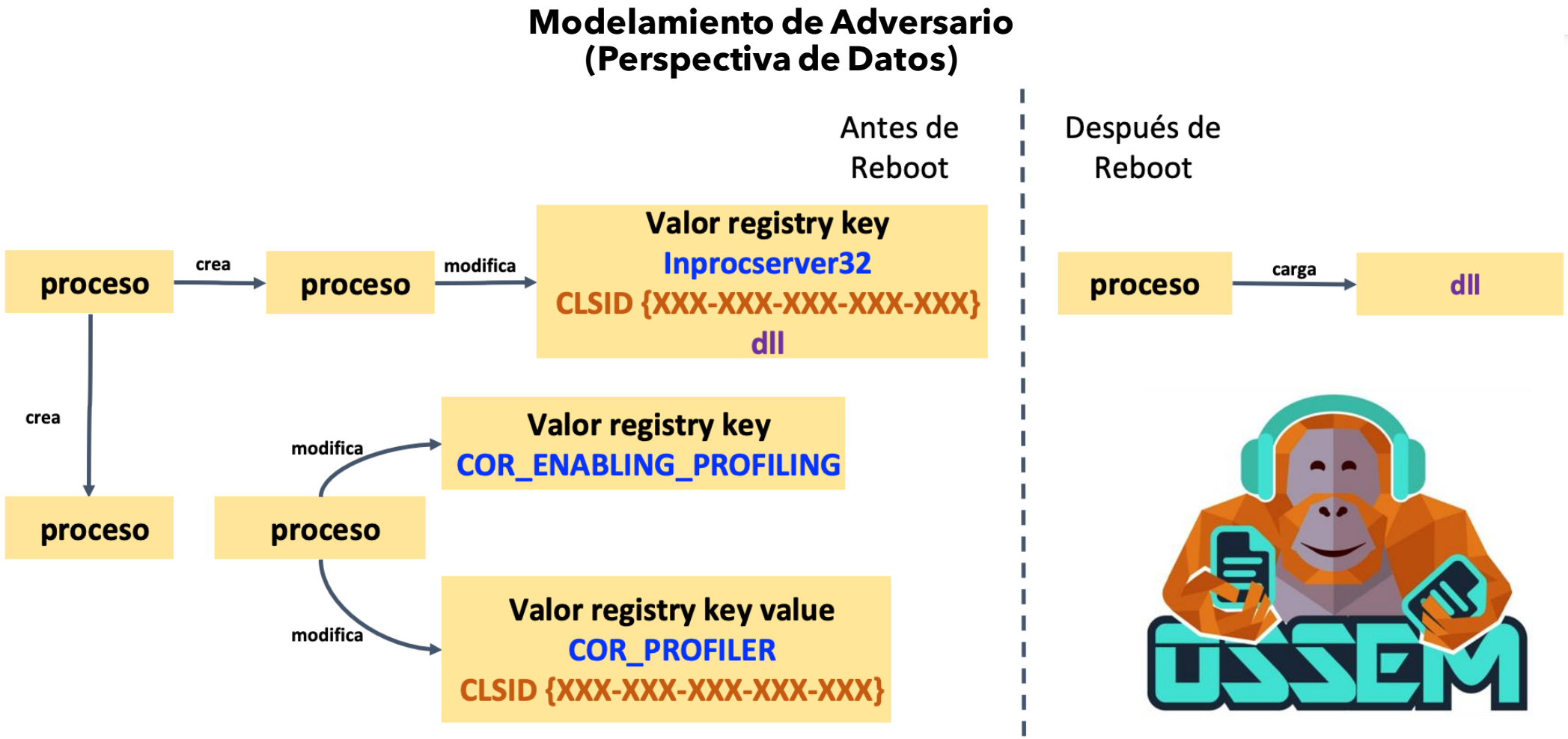
https://jupyter.org/

A Jupyter Notebook



https://jupyter.org/

Ejemplo: Modelando el uso de **COR_PROFILER**



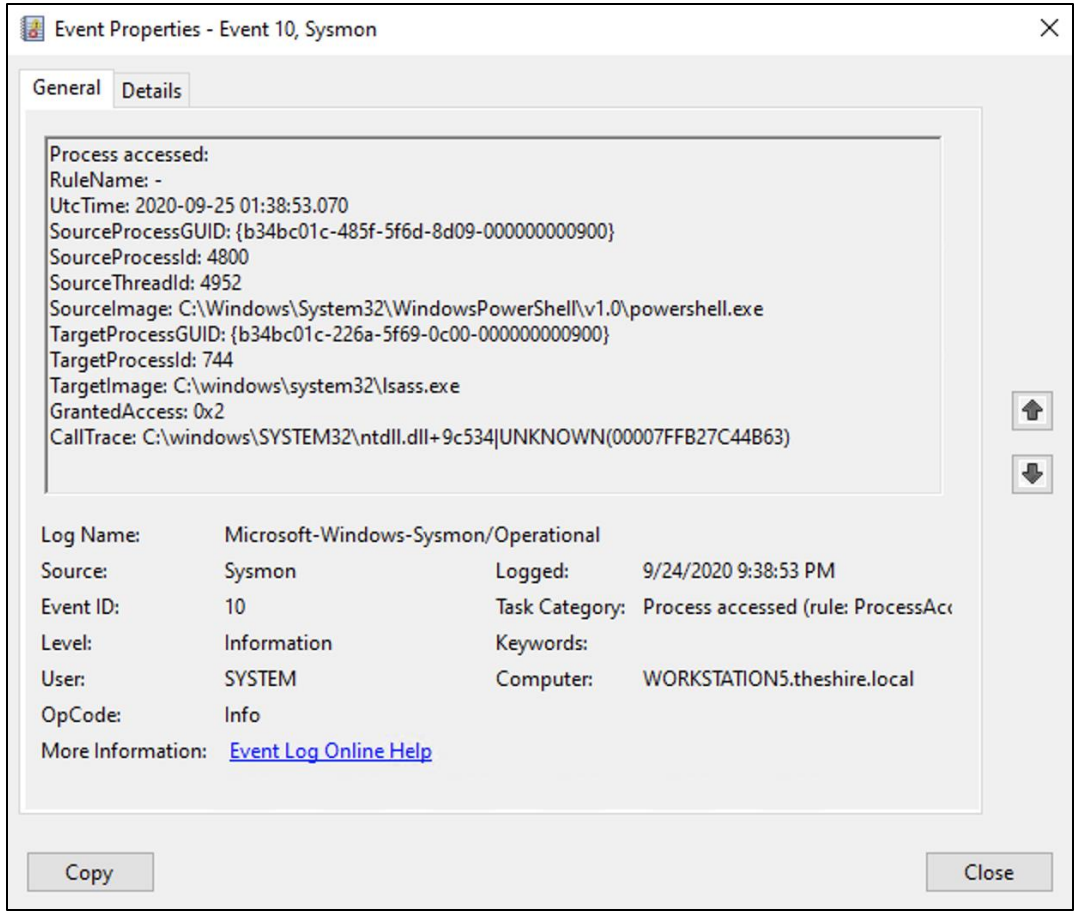
Ejemplo #1: Persistencia via COR_PROFILER

```
networkConnection = spark.sql(
'''
SELECT h.Image as ProcessNetwork, h.DestinationIp, g.ProcessLoadDll, g.ProcessModifyEnvironment,
       g.Environment, g.InprocserverProcess, g.TargetObject, g.Details
FROM coreProfilerExecution h
INNER JOIN
    (
    SELECT f.ProcessGuid, e.ProcessLoadDll, e.ProcessModifyEnvironment, e.Environment,
           e.InprocserverProcess, e.TargetObject, e.Details
    FROM coreProfilerExecution f
    INNER JOIN
        (
        SELECT d.ProcessGuid, d.Image as ProcessLoadDll, c.ProcessModifyEnvironment, c.Environment,
               c.InprocserverProcess, c.TargetObject, c.Details
        FROM coreProfilerExecution d
        INNER JOIN
            (
            SELECT b. Image as ProcessModifyEnvironment, b.TargetObject as Environment, b.Details as CLSID,
                   a.Image as InprocserverProcess, a.TargetObject, a.Details
            FROM coreProfilerSetup b
            INNER JOIN
                (
                SELECT Image, TargetObject, Details
                FROM coreProfilerSetup
                WHERE event_id = 13 AND lower(TargetObject) LIKE '%inprocserver%'
                ) a
            ON a.TargetObject LIKE CONCAT('%',b.Details,'%')
            WHERE b.event_id = 13 AND lower(b.TargetObject) LIKE '%cor_profiler%'
            ) c
        ON c.Details = d.ImageLoaded
        WHERE event_id = 7
        ) e
    ON e.ProcessGuid = f.ParentProcessGuid
    WHERE f.event_id = 1
    )g
ON g.ProcessGuid = h.ProcessGuid
WHERE event_id = 3
''')
```

```
-RECORD 0-------------------------------------------------------------------------------------------------------------------------------
 ProcessNetwork          | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\Hosts\
ServiceHub.Host.CLR.x86\ServiceHub.SettingsHost.exe
 DestinationIp           | 23.217.158.90
 ProcessLoadDll          | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\contro
ller\Microsoft.ServiceHub.Controller.exe
 ProcessModifyEnvironment | C:\WINDOWS\system32\wbem\wmiprvse.exe
 Environment             | HKU\S-1-5-21-579568221-2751777276-1469956634-1001\Environment\COR_PROFILER
 InprocserverProcess     | C:\WINDOWS\system32\reg.exe
 TargetObject            | HKU\S-1-5-21-579568221-2751777276-1469956634-1001_Classes\CLSID\{11111111-1111-1111-111
1-1111deadbeef}\InProcServer32\(Default)
 Details                 | C:\Users\jamie\Desktop\e0b3489da74f.dll
-RECORD 1-------------------------------------------------------------------------------------------------------------------------------
 ProcessNetwork          | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\Hosts\
ServiceHub.Host.CLR.x86\ServiceHub.IdentityHost.exe
 DestinationIp           | 40.126.2.2
 ProcessLoadDll          | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\contro
ller\Microsoft.ServiceHub.Controller.exe
 ProcessModifyEnvironment | C:\WINDOWS\system32\wbem\wmiprvse.exe
 Environment             | HKU\S-1-5-21-579568221-2751777276-1469956634-1001\Environment\COR_PROFILER
 InprocserverProcess     | C:\WINDOWS\system32\reg.exe
 TargetObject            | HKU\S-1-5-21-579568221-2751777276-1469956634-1001_Classes\CLSID\{11111111-1111-1111-111
1-1111deadbeef}\InProcServer32\(Default)
 Details                 | C:\Users\jamie\Desktop\e0b3489da74f.dll
-RECORD 2-------------------------------------------------------------------------------------------------------------------------------
 ProcessNetwork          | C:\Windows\System32\regsvr32.exe
 DestinationIp           | 67.199.248.10
 ProcessLoadDll          | C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\ServiceHub\contro
ller\Microsoft.ServiceHub.Controller.exe
 ProcessModifyEnvironment | C:\WINDOWS\system32\wbem\wmiprvse.exe
 Environment             | HKU\S-1-5-21-579568221-2751777276-1469956634-1001\Environment\COR_PROFILER
 InprocserverProcess     | C:\WINDOWS\system32\reg.exe
 TargetObject            | HKU\S-1-5-21-579568221-2751777276-1469956634-1001_Classes\CLSID\{11111111-1111-1111-111
1-1111deadbeef}\InProcServer32\(Default)
 Details                 | C:\Users\jamie\Desktop\e0b3489da74f.dll
```

https://jupyter.org/

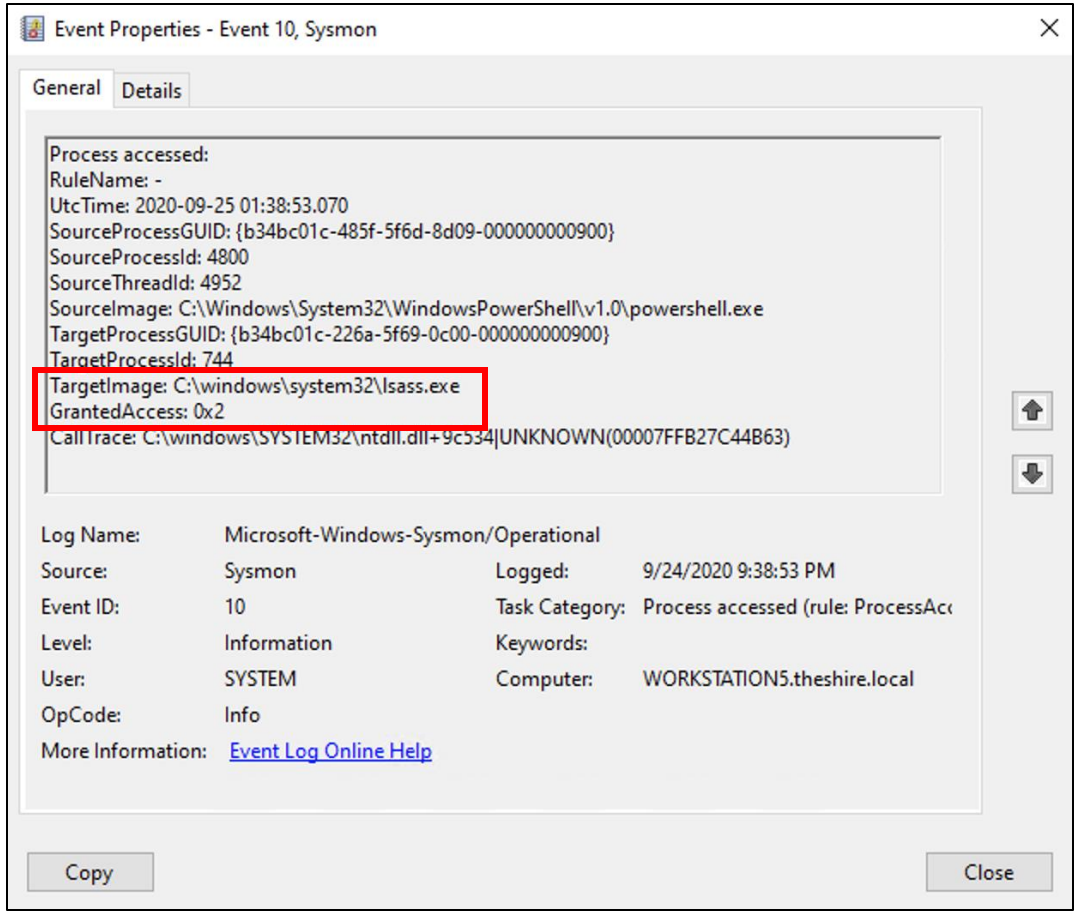
Ejemplo #2: Accesso a LSASS



PROCESS_CREATE_PROCESS (0x0080)	Required to create a process.
PROCESS_CREATE_THREAD (0x0002)	Required to create a thread.
PROCESS_DUP_HANDLE (0x0040)	Required to duplicate a handle using **DuplicateHandle**.
PROCESS_QUERY_INFORMATION (0x0400)	Required to retrieve certain information about a process, such as its token, exit code, and priority class (see **OpenProcessToken**).
PROCESS_QUERY_LIMITED_INFORMATION (0x1000)	Required to retrieve certain information about a process (see **GetExitCodeProcess**, **GetPriorityClass**, **IsProcessInJob**, **QueryFullProcessImageName**). A handle that has the **PROCESS_QUERY_INFORMATION** access right is automatically granted **PROCESS_QUERY_LIMITED_INFORMATION**.**Windows Server 2003 and Windows XP:** This access right is not supported.

https://docs.microsoft.com/en-us/windows/win32/procthread/process-security-and-access-rights

Ejemplo #2: Accesso a LSASS



PROCESS_CREATE_PROCESS (0x0080)	Required to create a process.
PROCESS_CREATE_THREAD (0x0002)	Required to create a thread.
PROCESS_DUP_HANDLE (0x0040)	Required to duplicate a handle using **DuplicateHandle**.
PROCESS_QUERY_INFORMATION (0x0400)	Required to retrieve certain information about a process, such as its token, exit code, and priority class (see **OpenProcessToken**).
PROCESS_QUERY_LIMITED_INFORMATION (0x1000)	Required to retrieve certain information about a process (see **GetExitCodeProcess**, **GetPriorityClass**, **IsProcessInJob**, **QueryFullProcessImageName**). A handle that has the **PROCESS_QUERY_INFORMATION** access right is automatically granted **PROCESS_QUERY_LIMITED_INFORMATION**.**Windows Server 2003 and Windows XP:** This access right is not supported.

https://docs.microsoft.com/en-us/windows/win32/procthread/process-security-and-access-rights

Que tipos de análisis podemos desarrollar?

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)>
```

Transformación de Datos

https://infosecjupyterbook.com/community-workshops/defcon_btv_2020/use-cases/01_Data_Analysis_Process_Injection.html

Que tipos de análisis podemos desarrollar?

- Apply the Spark UDF

```
processAccessRights = spark.sql(
'''
SELECT GrantedAccess, getAccessRights(GrantedAccess) as RightsRequested, count(*) as Count
FROM processInjection
WHERE lower(Channel) LIKE '%sysmon%'
    AND EventID = 10
GROUP BY GrantedAccess, RightsRequested
ORDER BY Count DESC
''')

print('This dataframe has {} records!!'.format(processAccessRights.count()))
processAccessRights.show(truncate = 80)
```

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

Seleccion y Resumen de Datos

https://infosecjupyterbook.com/community-workshops/defcon_btv_2020/use-cases/01_Data_Analysis_Process_Injection.html

Que tipos de análisis podemos desarrollar?

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)
```

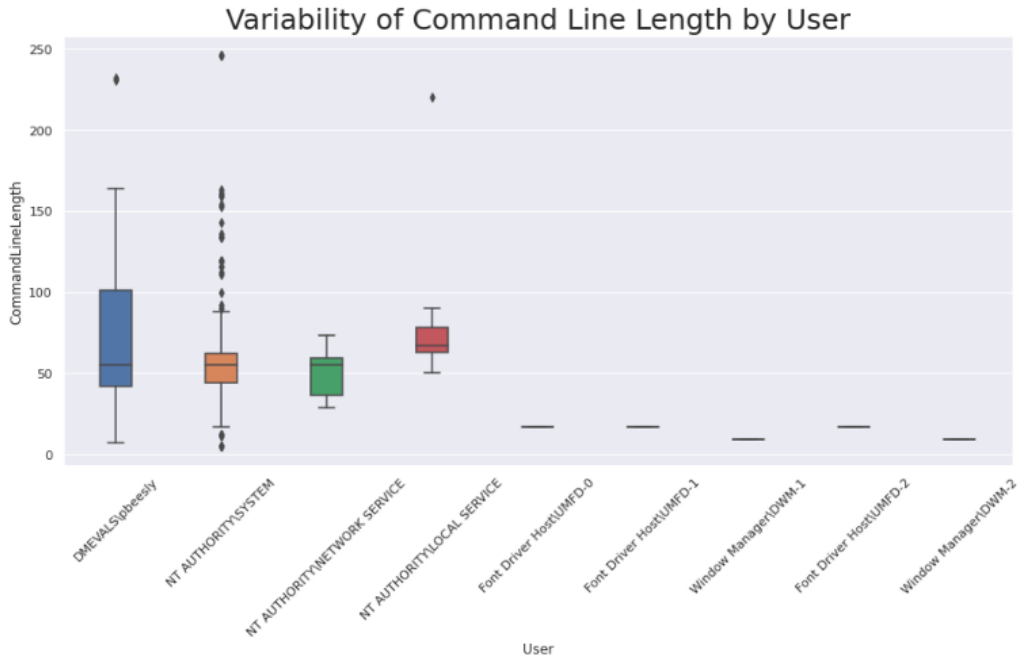
```
This dataframe has 88 records!!
+----------------------------------------+----------------------------+-----------+
|                              SourceImage|                 TargetImage|NewThreadId|
+----------------------------------------+----------------------------+-----------+
|C:\windows\System32\WindowsPowerShell...|C:\windows\system32\notepad.exe|       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|
```

Correlación de Datos

https://infosecjupyterbook.com/community-workshops/defcon_btv_2020/use-cases/01_Data_Analysis_Process_Injection.html

Que tipos de análisis podemos desarrollar?

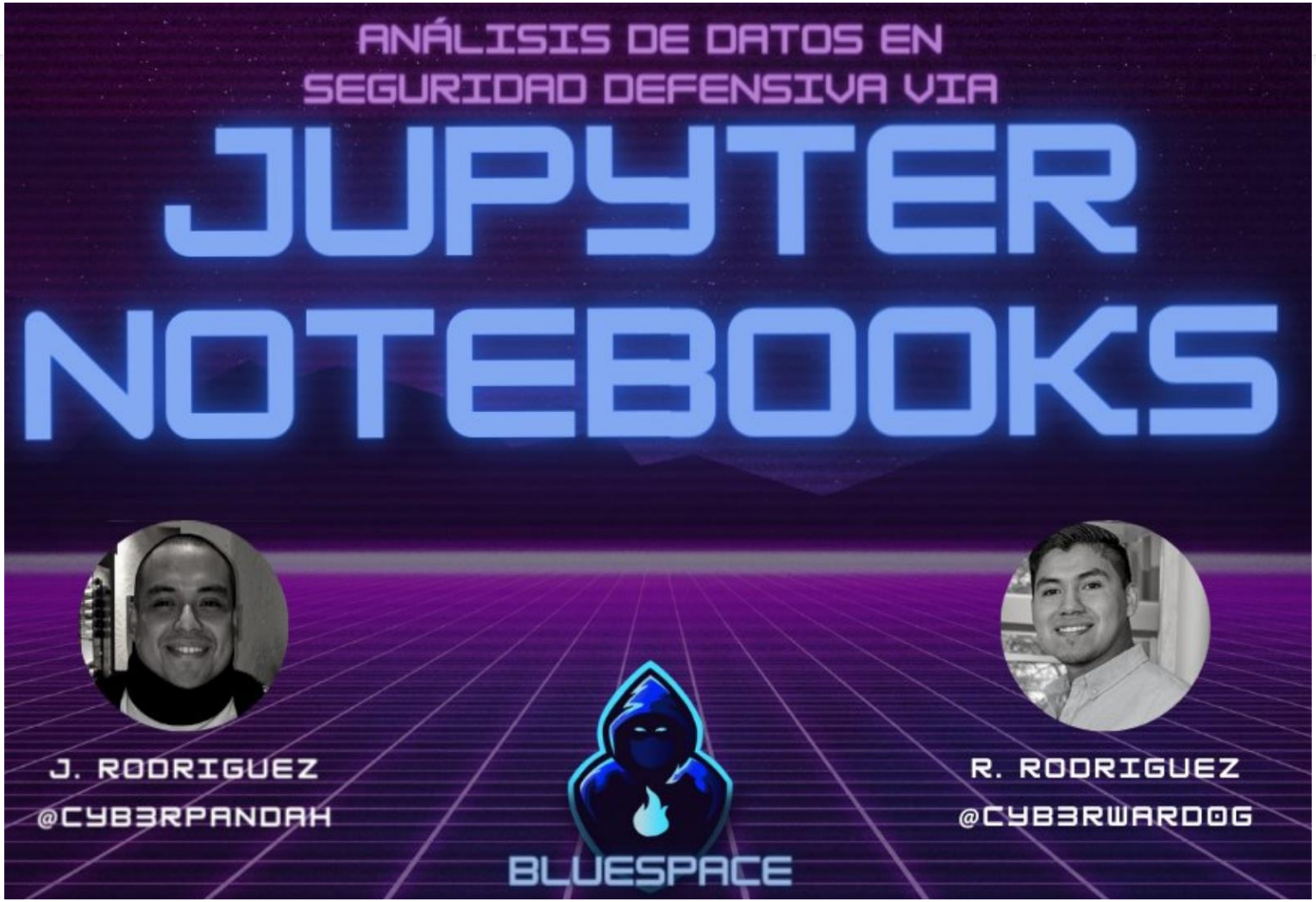
```
# Source of Data
source = commandLineLength.toPandas()

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

# 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);
```



Visualización de Datos

https://infosecjupyterbook.com/community-workshops/defcon_btv_2020/use-cases/01_Data_Analysis_Process_Injection.html

Jupyter Notebooks: Septiembre 26 @15:00-17:00




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

Validación y Documentación de Estrategia

Contando la historia detrás del resultado

Download & Process Mordor File

```
mordor_file = "https://raw.githubusercontent.com/OTRF/mordor/master/datasets/small/wir
registerMordorSQLTable(spark, mordor_file, "mordorTable")
```

Analytic I

FP Rate	Log Channel	Description
Medium	['Microsoft-Windows-Sysmon/Operational']	Look for the creation of Event consumers type.

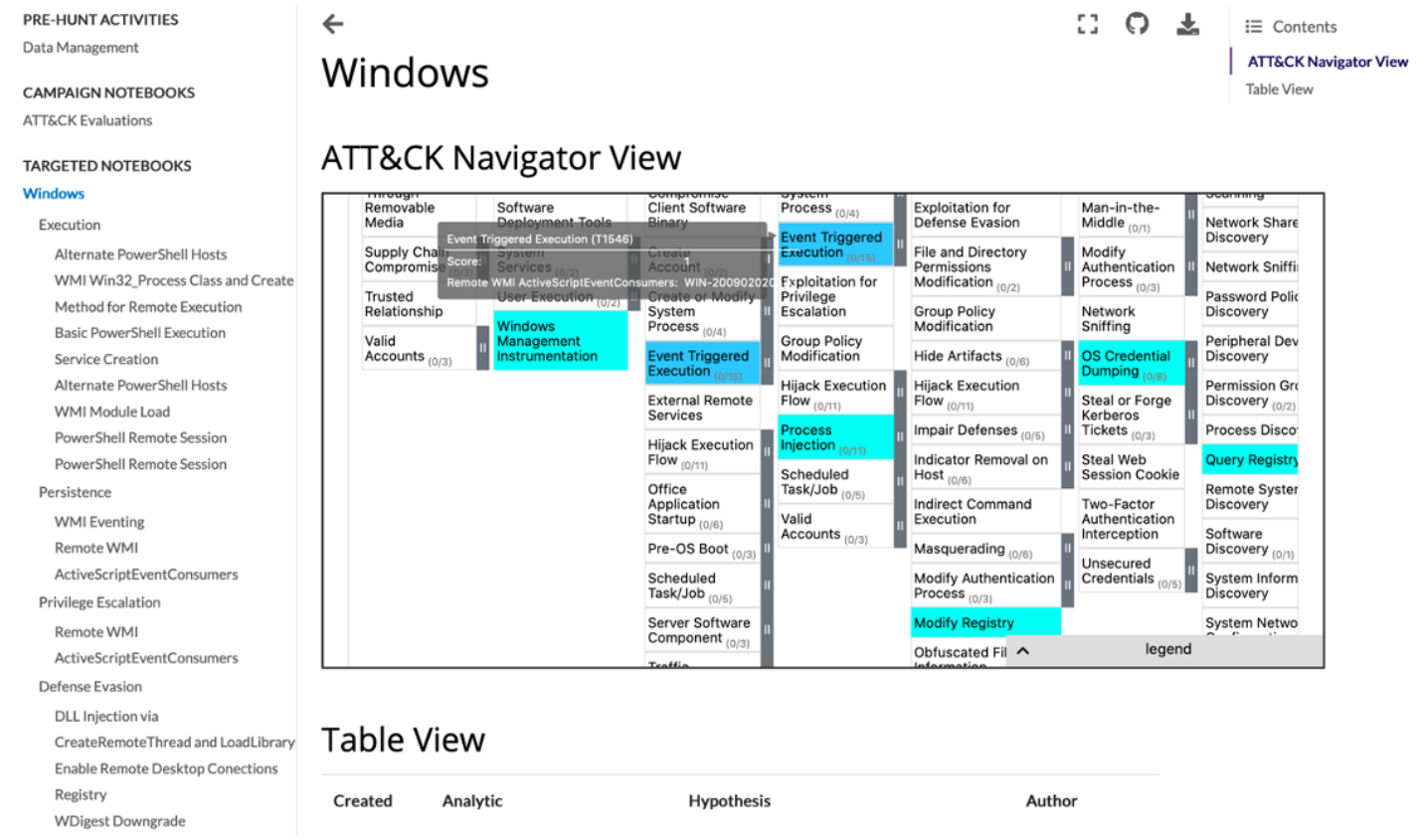
```
df = spark.sql(
    '''
SELECT EventID, EventType
FROM mordorTable
WHERE Channel = 'Microsoft-Windows-Sysmon/Operational'
  AND EventID = 20
  AND LOWER(Message) Like '%type: script%'
    '''
)
df.show(10,False)
```

ThreatHunter-Playbook

- Conjunto de Notebooks que colaboran con el desarrollo de tecnicas e hipotesis en investigacion de detecciones.
- Este proyecto documenta estrategias en forma de **notebooks interactivos**, con el objetivo de proveer los resultados de la investigacion en forma sencilla y flexible.
- Cada notebooks interactúa con un set de datos del proyecto **Mordor** 😈

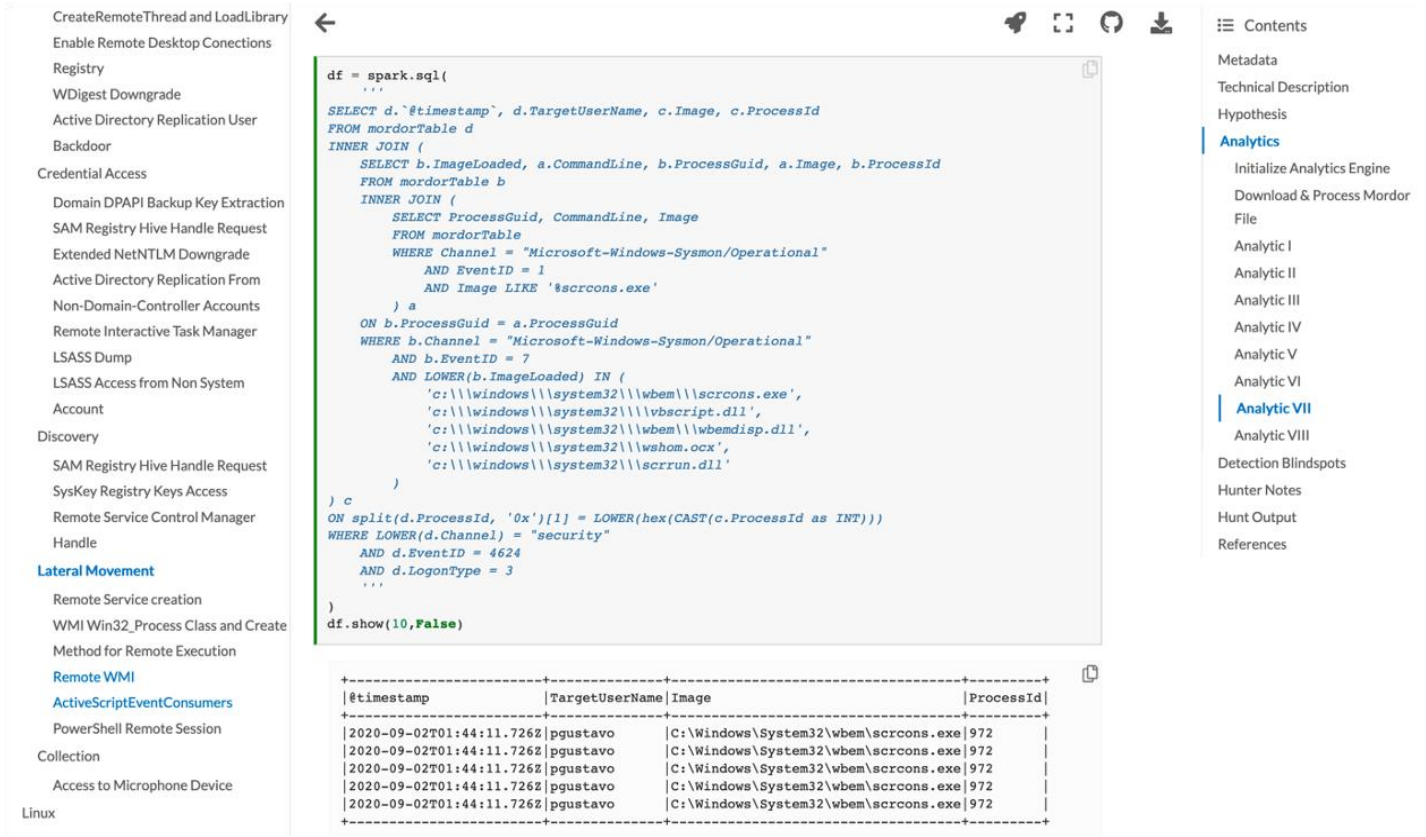
https://threathunterplaybook.com/introduction.html

Playbooks estan mapeados a **ATT&CK**

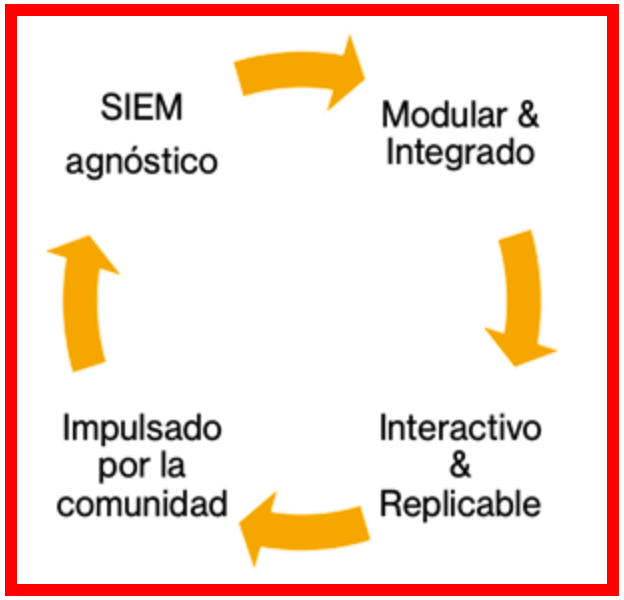


https://threathunterplaybook.com/notebooks/windows/windows.html

Documentación y Validación de Analíticos con Sets de datos del proyecto **Mordor**



https://threathunterplaybook.com/notebooks/windows/windows.html


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

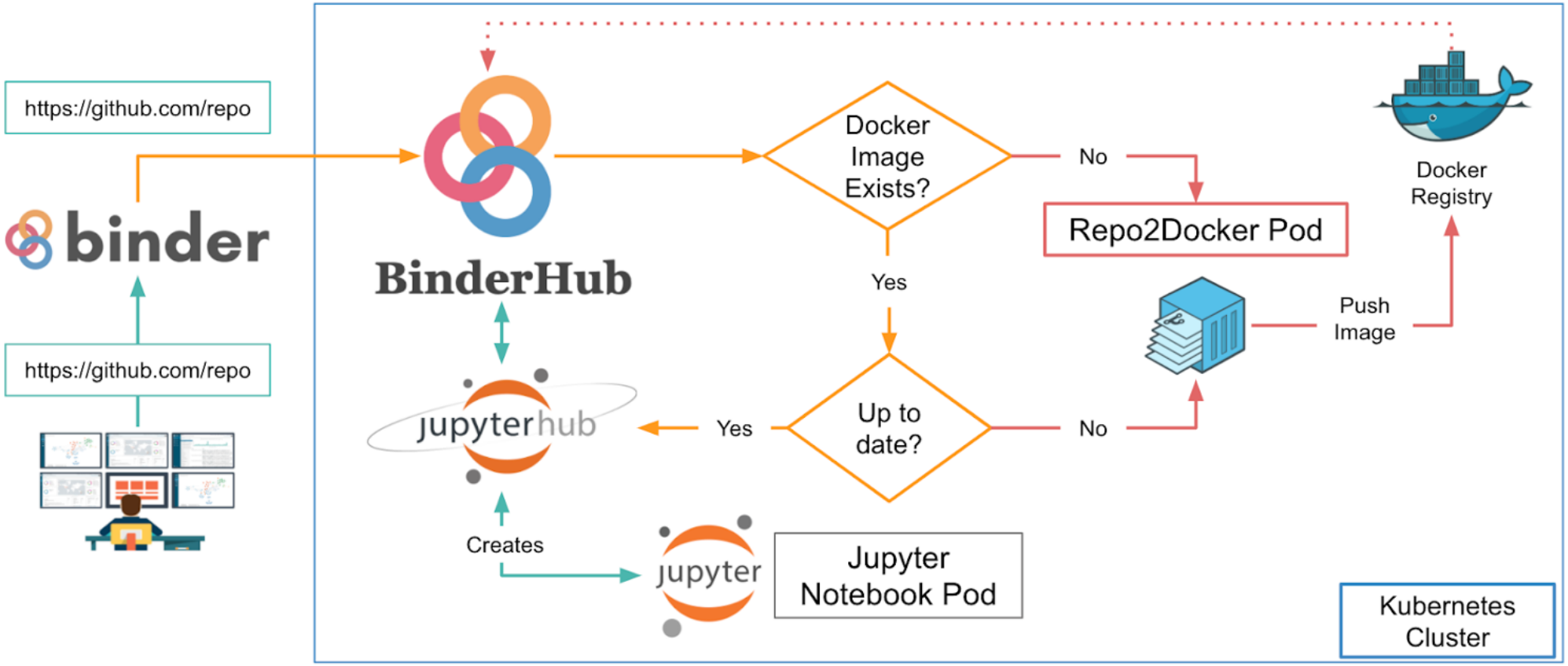

Resumir
Filtrar
Correlacionar
Visualizar


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

Compartiendo con la Comunidad

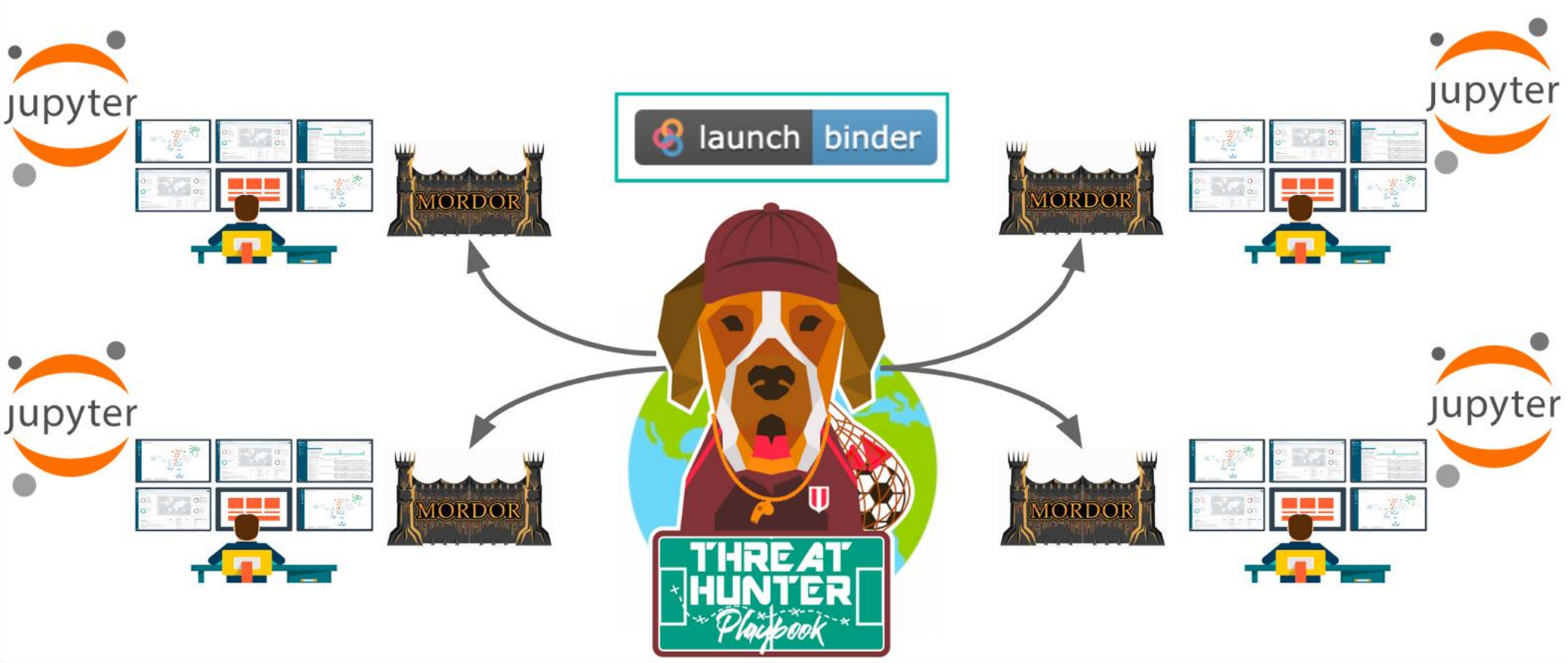
En forma práctica, interactiva y replicable

Replicable? Práctico? Interactivo?



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

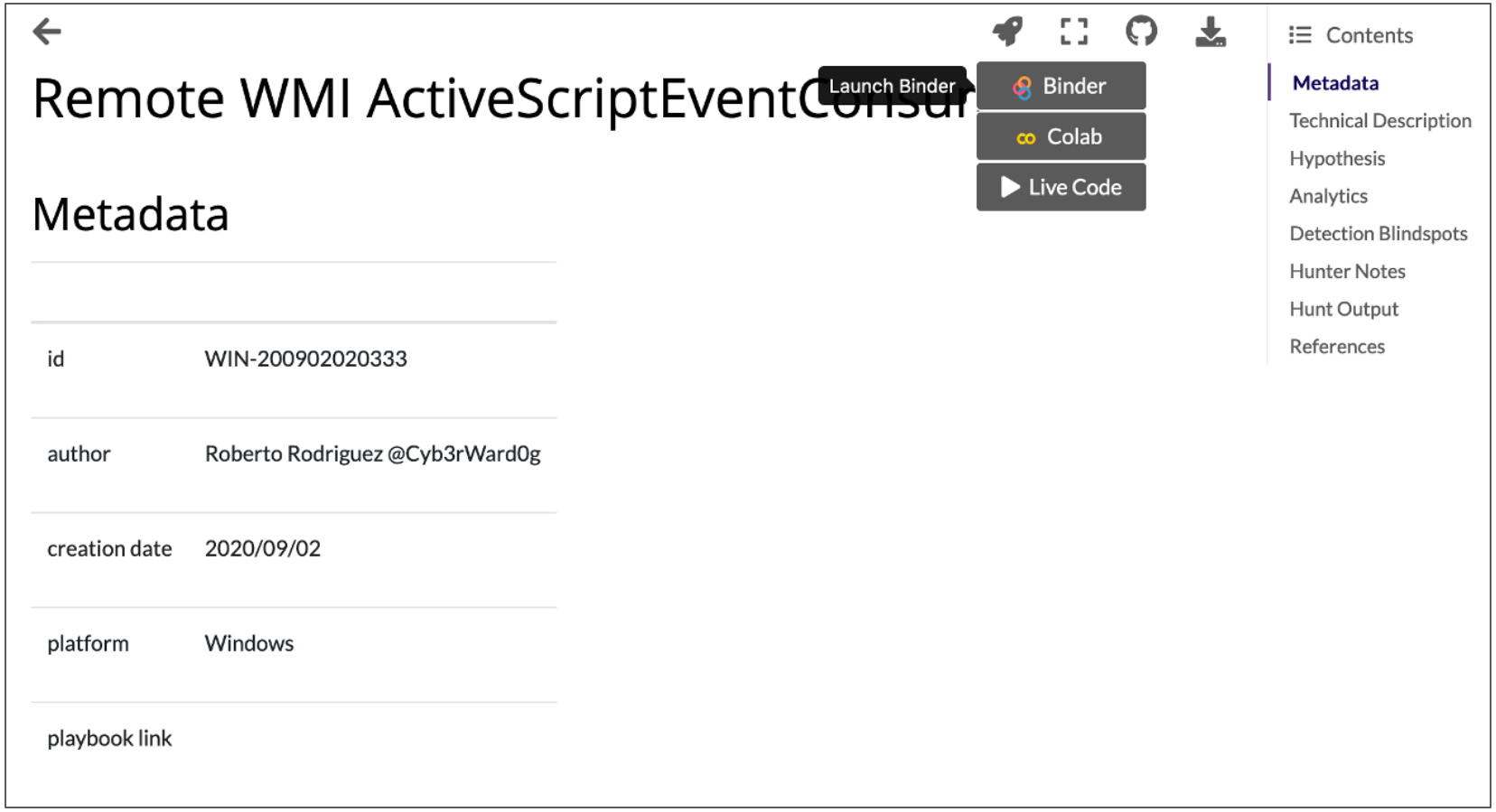
Replicable? Práctico? Interactivo?



Replicable? Práctico? Interactivo?

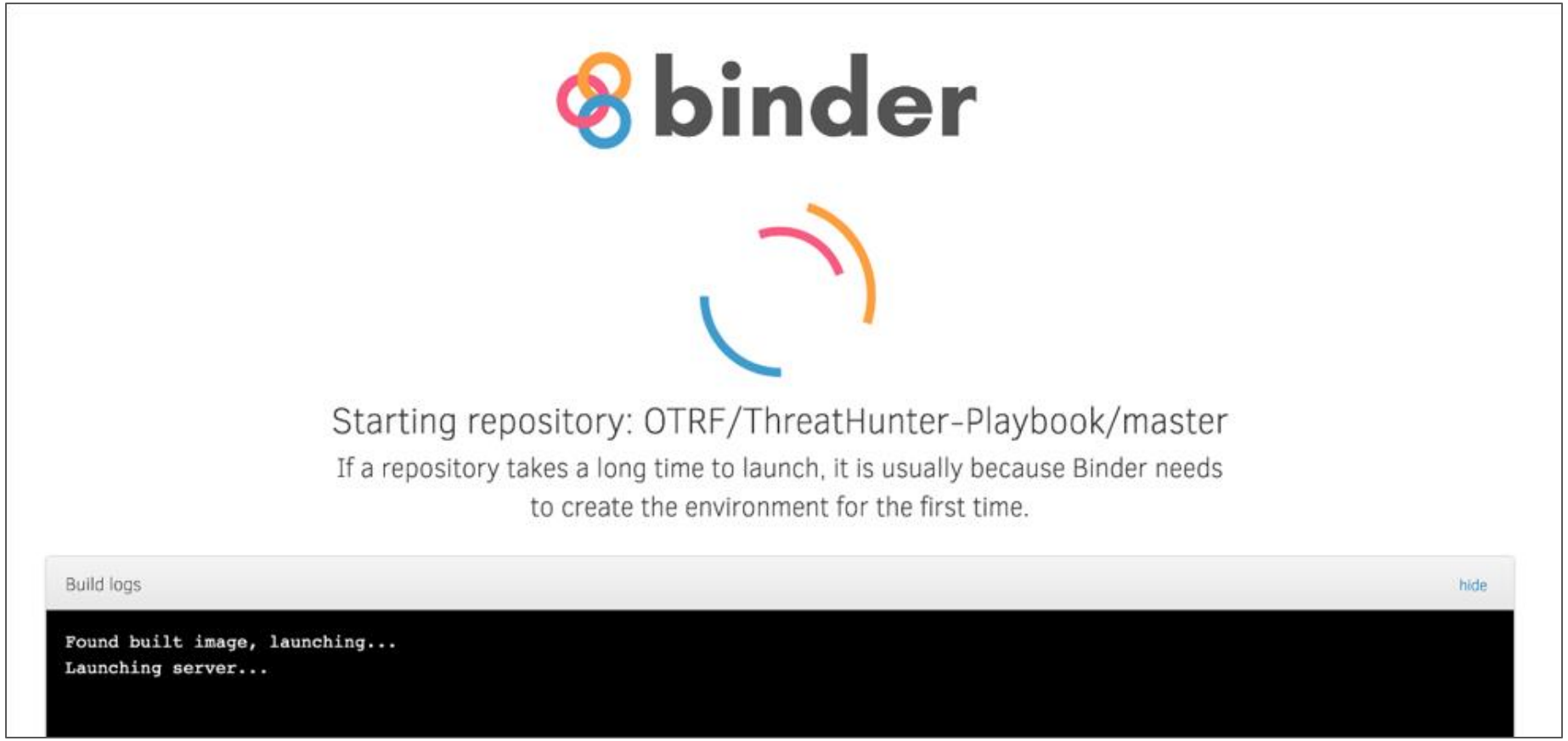
https://twitter.com/HunterPlaybook/status/1301207718355759107

Replicable? Práctico? Interactivo?



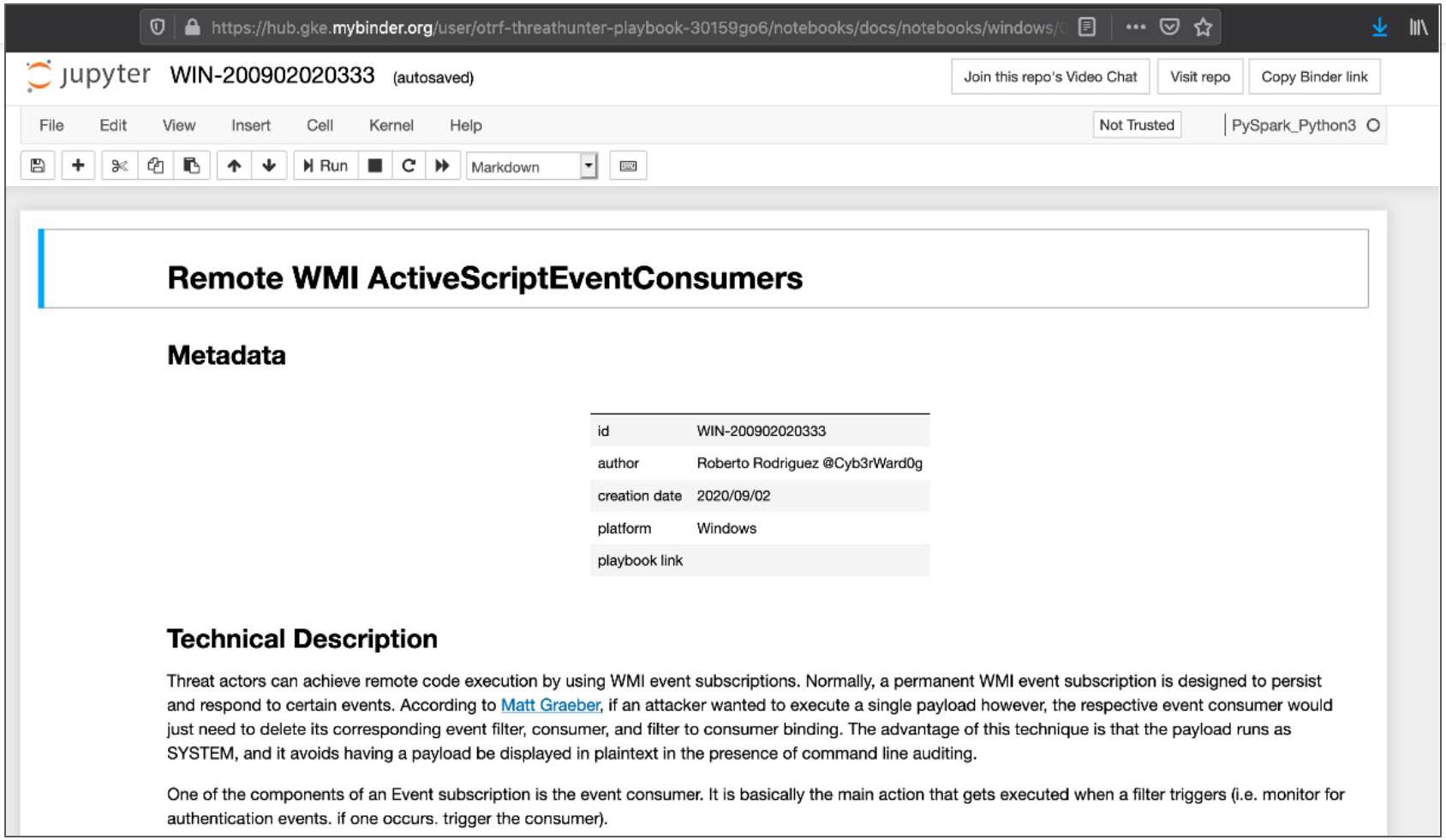
https://threathunterplaybook.com/notebooks/windows/08_lateral_movement/WIN-200902020333.html

Replicable? Práctico? Interactivo?



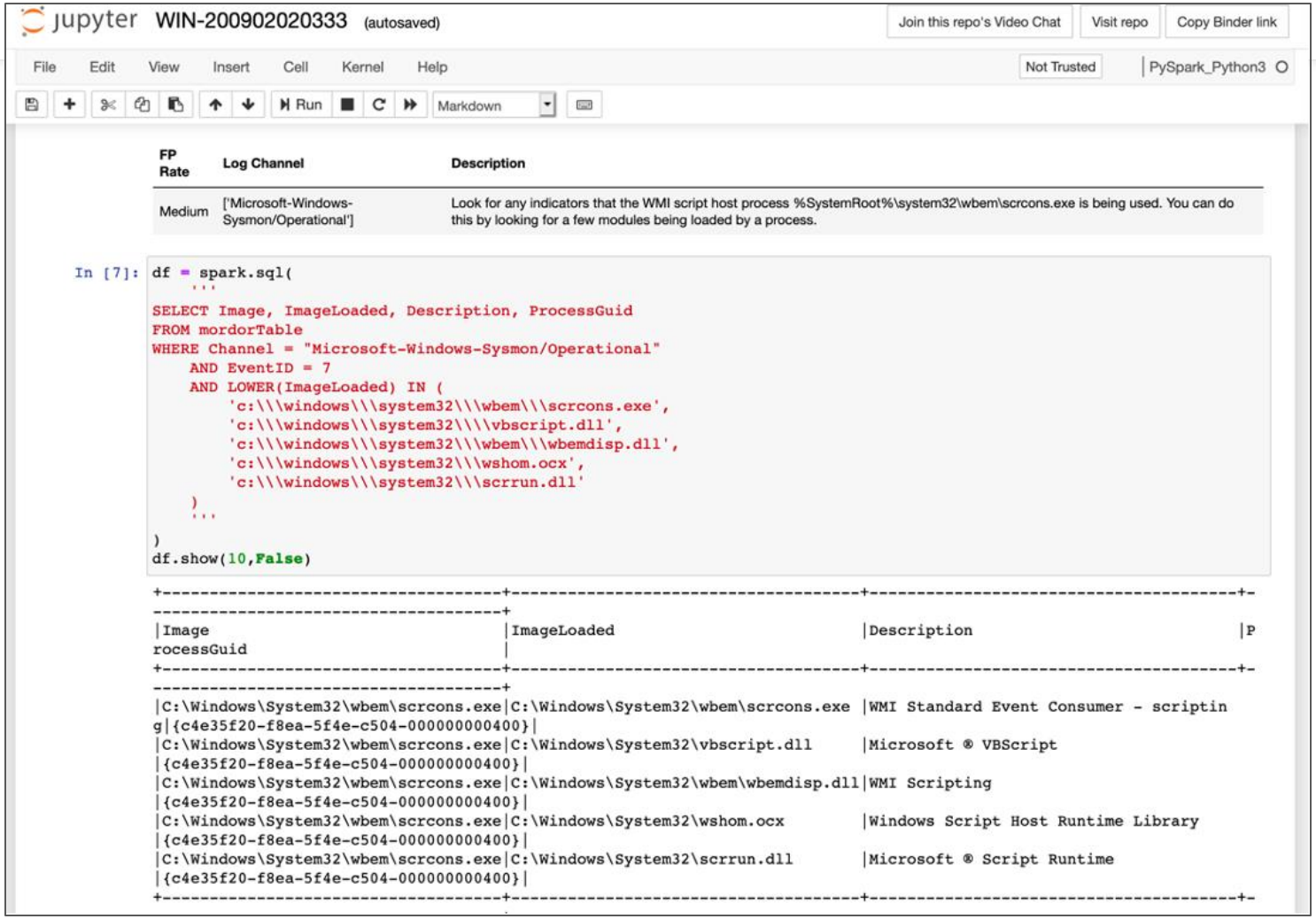
https://threathunterplaybook.com/notebooks/windows/08_lateral_movement/WIN-200902020333.html

Replicable? Práctico? Interactivo?



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

Replicable? Práctico? Interactivo?



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

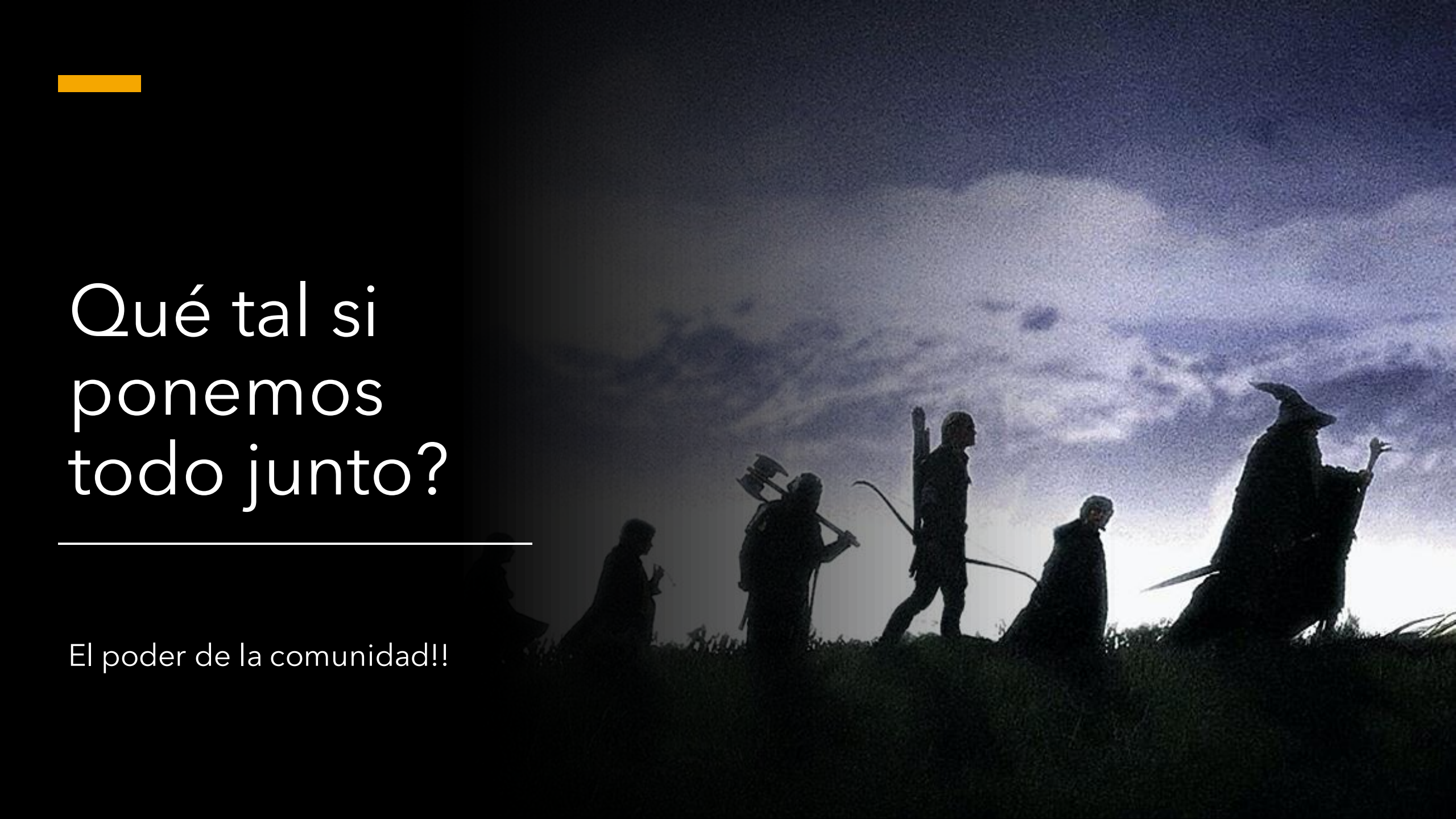
Puedes Generar Impacto Siendo tu Mismo!

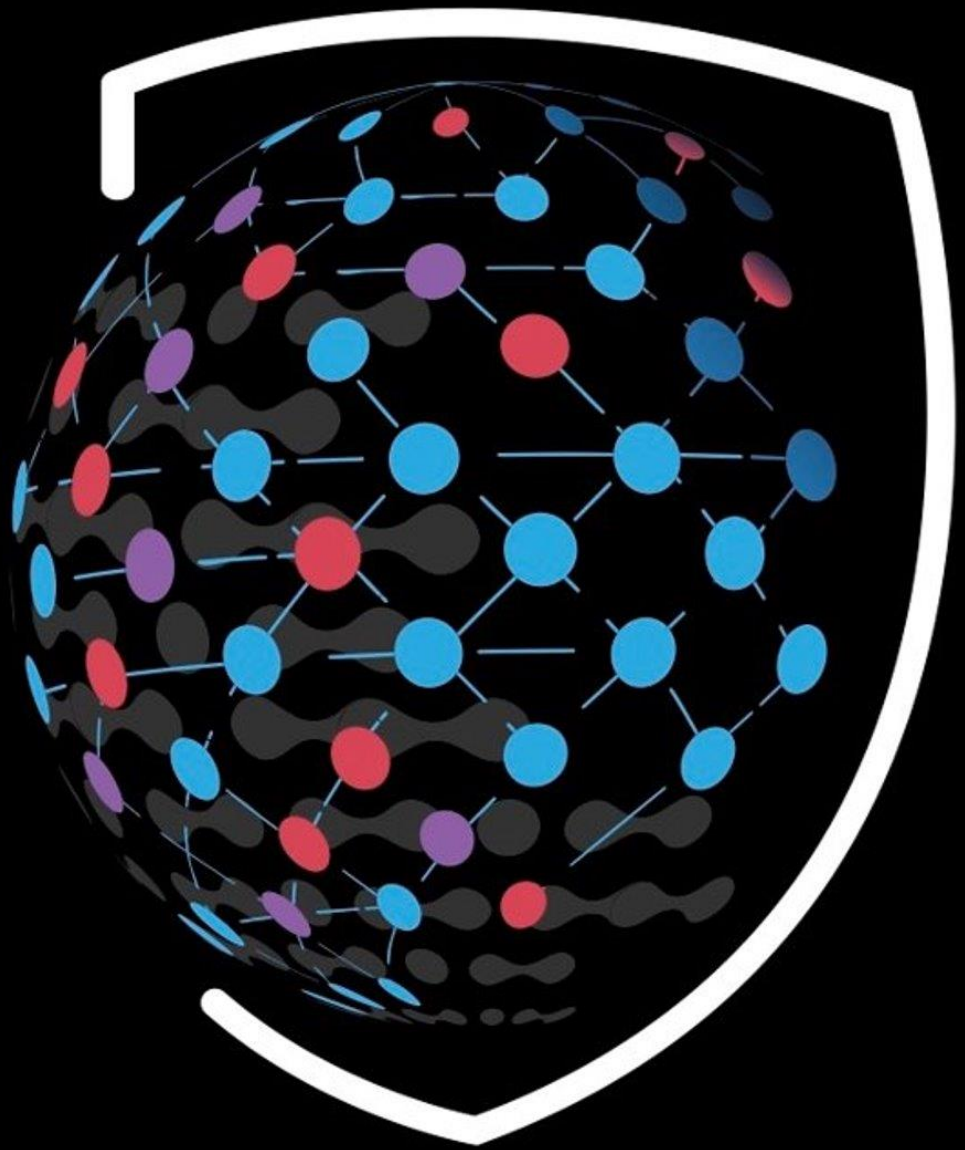
"Don't worry about being the next me. Be the first you"

Dwayne 'The Rock' Johnson

Qué tal si ponemos todo junto?

El poder de la comunidad!!





OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY


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

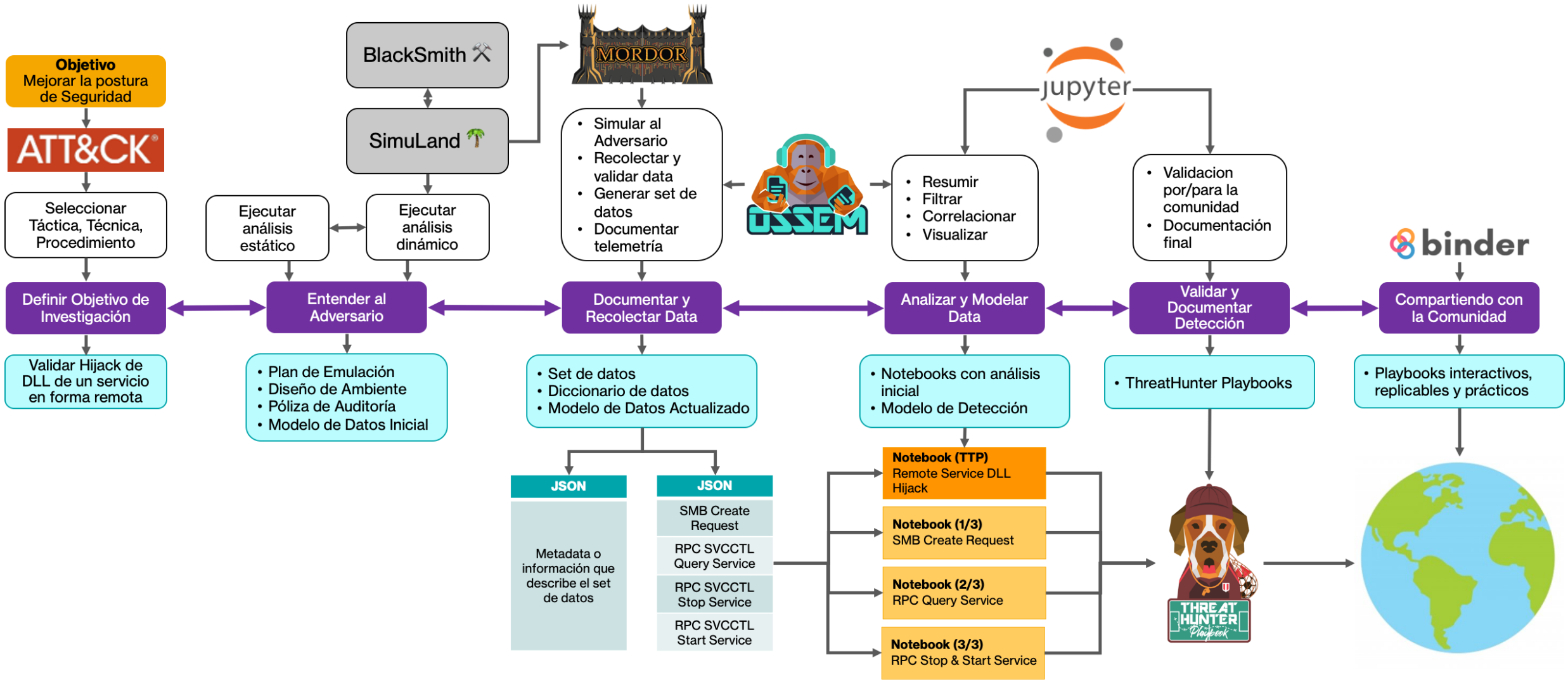

Definir un Objetivo de Investigación
Entender la Estrategia del Adversario
Recolectar y Documentar Data
Analizar y Modelar Data
Validación y Documentación de Estrategia de Detección
Compartir la Investigación


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

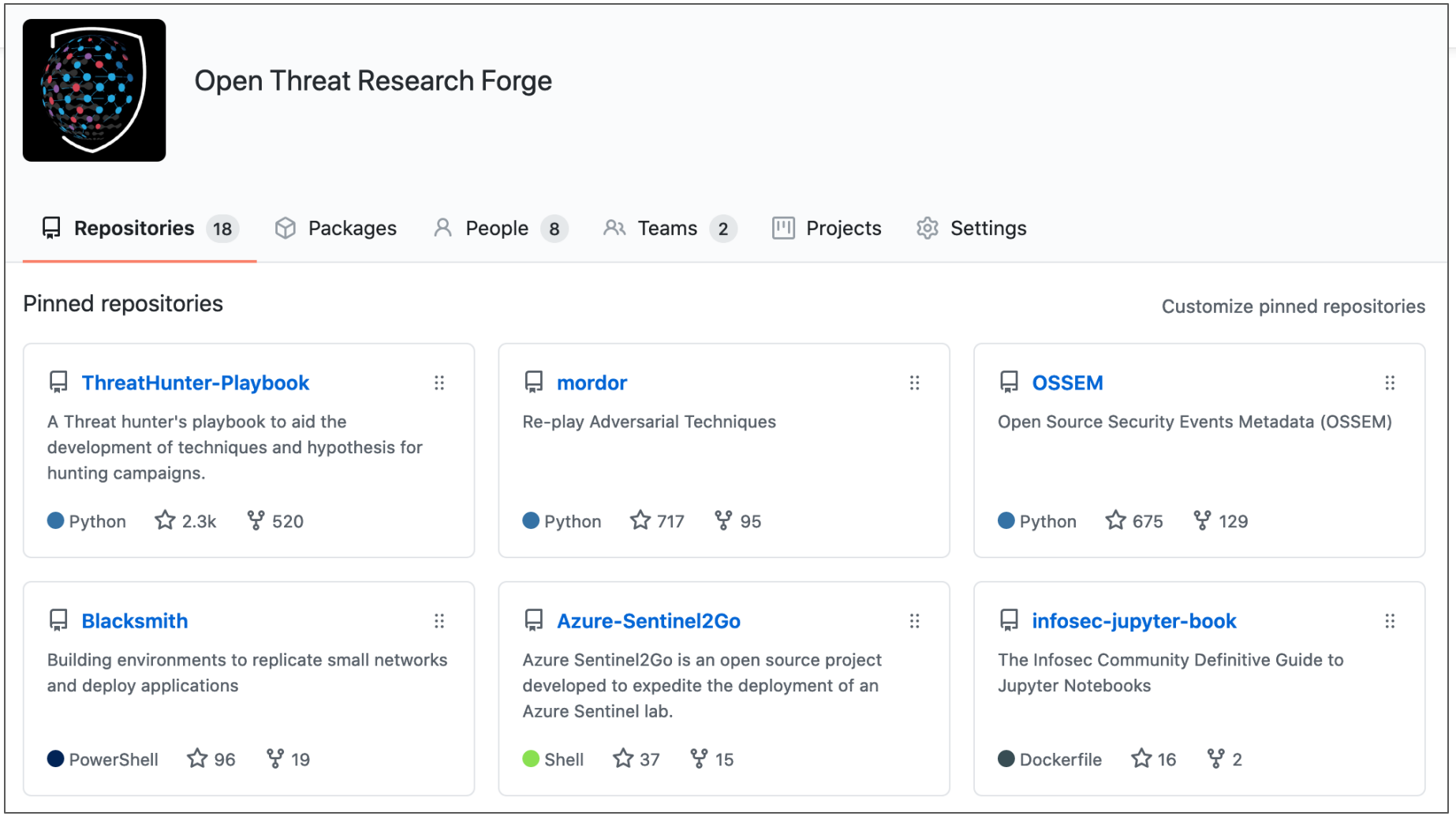

Contexto de Seguridad
Notas y Entregables de Investigación
Eventos de Seguridad
Analíticos


Resumir
Filtrar
Correlacionar
Visualizar


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


Objetivo
Mejorar la postura de Seguridad
ATT&CK
Seleccionar Táctica, Técnica, Procedimiento
Definir Objetivo de Investigación
Validar Hijack de DLL de un servicio en forma remota
BlackSmith
SimuLand
Ejecutar análisis estático
Ejecutar análisis dinámico
Entender al Adversario
• Plan de Emulación
• Diseño de Ambiente
• Póliza de Auditoría
• Modelo de Datos Inicial
MORDOR
• Simular al Adversario
• Recolectar y validar data
• Generar set de datos
• Documentar telemetría
Documentar y Recolectar Data
• Set de datos
• Diccionario de datos
• Modelo de Datos Actualizado
JSON
Metadata o información que describe el set de datos
JSON
SMB Create Request
RPC SVCCTL Query Service
RPC SVCCTL Stop Service
RPC SVCCTL Start Service
jupyter
• Resumir
• Filtrar
• Correlacionar
• Visualizar
Analizar y Modelar Data
• Notebooks con análisis inicial
• Modelo de Detección
Notebook (TTP)
Remote Service DLL Hijack
Notebook (1/3)
SMB Create Request
Notebook (2/3)
RPC Query Service
Notebook (3/3)
RPC Stop & Start Service
• Validacion por/para la comunidad
• Documentación final
Validar y Documentar Detección
• ThreatHunter Playbooks
THREAT HUNTER
binder
Compartiendo con la Comunidad
• Playbooks interactivos, replicables y prácticos

https://github.com/OTRF

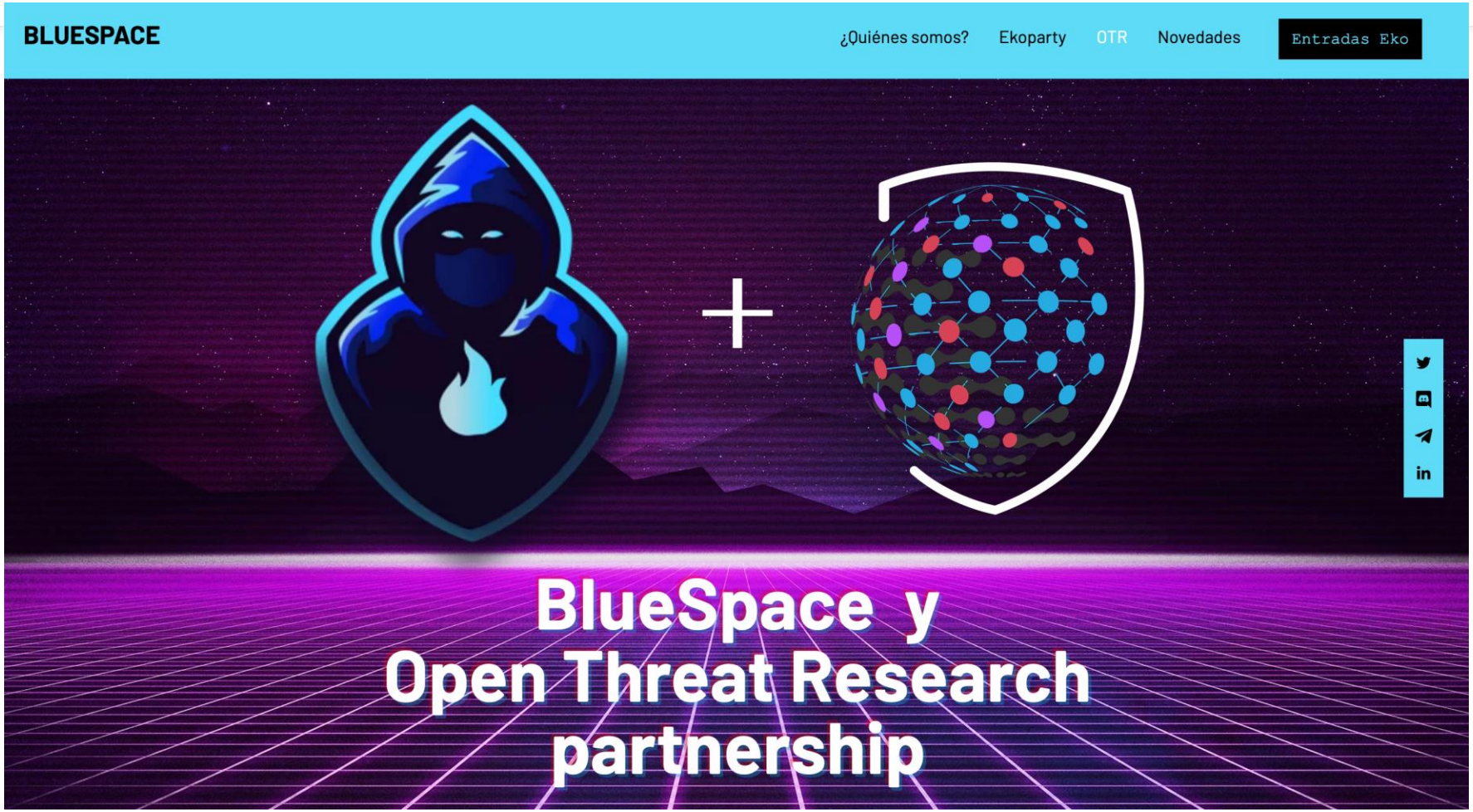


OTR Discord Disponible 

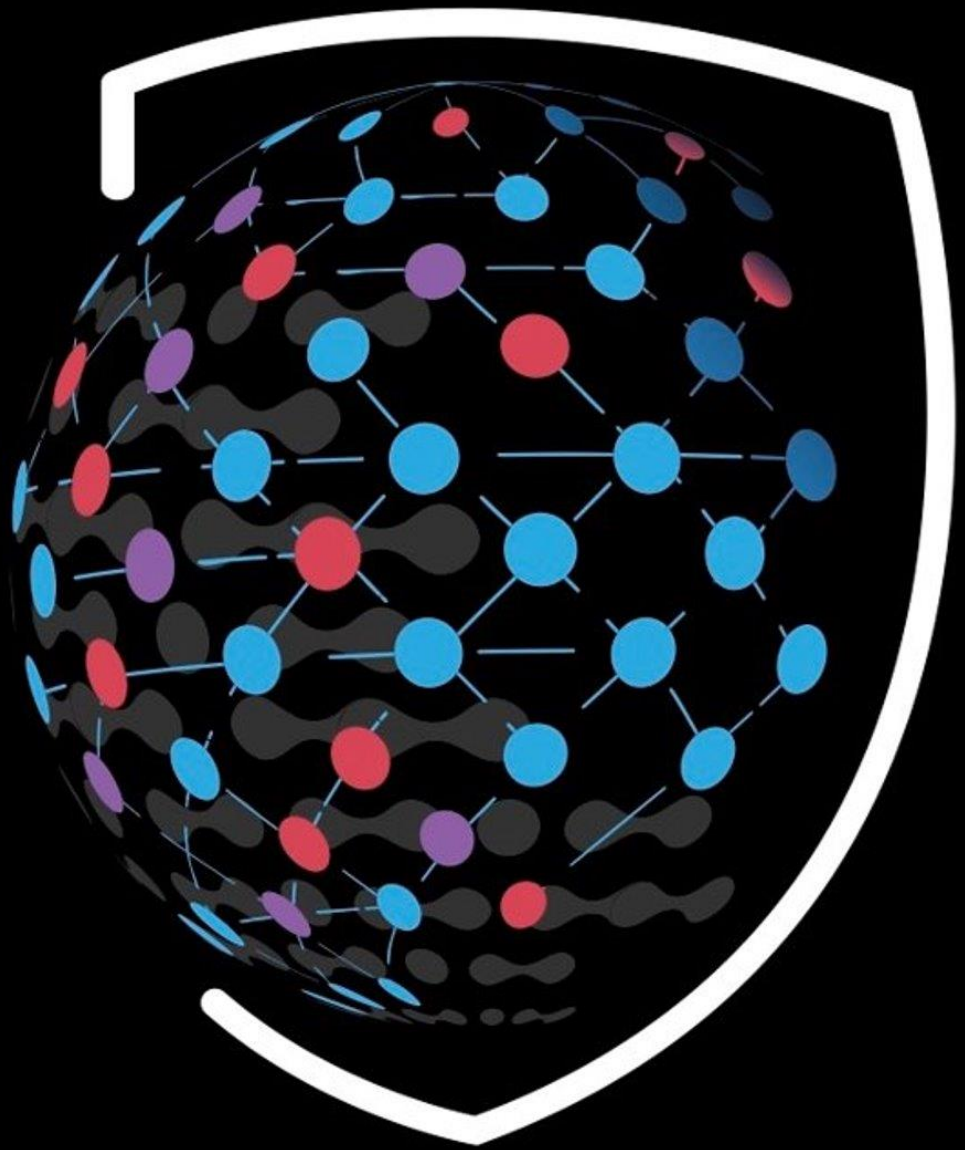
bitly.com/OTRDiscord

- Acepta el CAPTCHA
- Lee y acepta el código de conducta de nuestro discord
- Empezemos a colaborar y a compartir con la comunidad!

Partnership con el BlueSpace



https://www.bluespacesec.org/otr



OPEN THREAT RESEARCH

EMPOWERING THE INFOSEC COMMUNITY