Cyber Risk Advisory

28 de octubre de 2022

ESTANDARIZACIÓN PROYECTOS MITRE

CyberRisk Advisory



*ÍNDICE*

*1. Detection Categories MITRE*

*2. Obtener TTPs del cliente*

*3. Obtener la cobertura de cada TTP*

*4. Concatenarlas con las de la fuente que usen (ya sea Palo Alto…etc).*

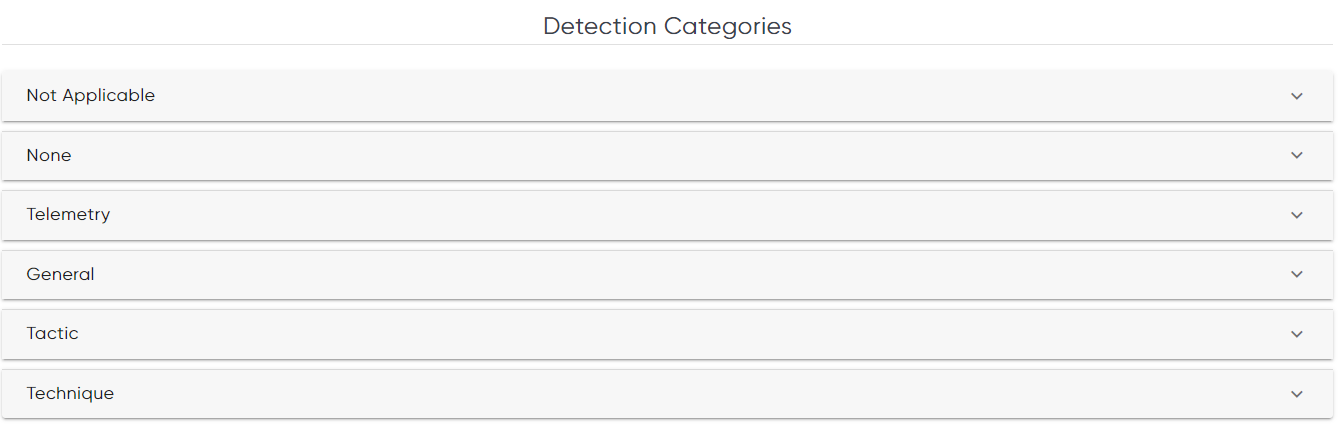
*5. MITRE NAVIGATOR*

*6. Obtención heatmaps*

*7. Score estandarizado*

1. Detection Categories MITRE

**Mitre Engenuity** distingue entre varias categorías de detección. Not aplicable, None, Telemetry, General, Tactic y Technique. Para nuestro análisis, nosotros bajaremos al nivel más bajo, que se corresponde con **Technique**.



Mas info: [ATT&CK® Evaluations (mitre-engenuity.org)](https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-sandworm/detection-categories)

Las técnicas representan cómo un adversario logra un objetivo táctico al realizar una acción. Para una misma táctica, hay una seria de técnica distintas, así como para una misma técnica, puede a ver varias formas distintas de implementarlo, a estas se les denomina subtecnicas.

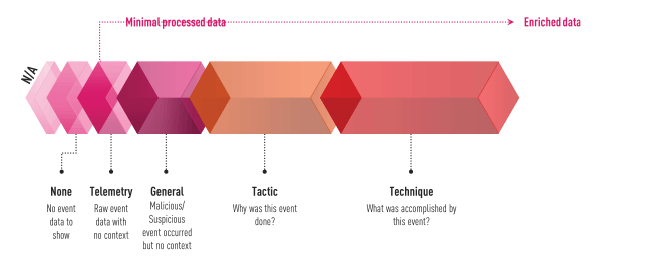
1. Obtener TTPs del cliente

En primer lugar, se categorizarán los casos de uso proporcionados por el cliente en la matriz de Mitre. Obteniendo así una seria de TTPs con su correspondiente ID.

Una TTP se refiere a Tactics, Techniques, and Procedures (TTPs). Y son comportamientos, métodos o patrones de actividad utilizados por un actor de amenazas o un grupo de actores de amenazas.

El proceso se hará por medio de un Excel. Y con el siguiente formato:

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre técnico/subtécnica | ID técnica/subtécnica | Entorno | Cobertura |
| External Remote Services | T1133 | Qradar | [0-4] Un número entre 0 y 4 (los decimales se redondean) |



1. Obtener la cobertura de cada TTP

*Para obtener la cobertura de cada TTP, habrá que realizar los siguiente pasos:*

* *En primer lugar, sacar el número de TTPs totales. Es decir el número de veces que aparece una TTP en nuestra categorización.*
* *Una vez obtenido lo anterior, se hará la siguiente regla. Si el numero de veces que aparece una TTP es mayor o igual a 4, el valor dado será de 0,5, en cambio si es inferior, se le asignará 0,25:*

*IF((CeldadelnumerodevecesdeesaTTP)>=4;0,5:0,25)*

1. Concatenarlas con las de la fuente que usen (ya sea Palo Alto…etc).

Una vez obtenido el valor de cada TTP, se juntarán con las de la fuente usada por el cliente. Es decir, si usa Palo Alto, hay una serie de TTP que Palo alto cubre y no es necesario categorizar, ya que ya las tenemos. **UNICAMENTE SE DEBERAN SELECCIONAR AQUELLAS TTPs QUE TENGAN VALOR 1.**

Por lo que si hay una TTP que nosotros tenemos categorizada y aparece en la fuente de e.g. Palo alto, borraremos nuestra categorización y su correspondiente valor y se dejara para que quede de la siguiente forma (SIEMPRE VALOR 1):



Se deberá también cambiar el nombre de “Technique” por el del EDR usado. Ya sea Qradar, Cortex ….etc

1. MITRE NAVIGATOR

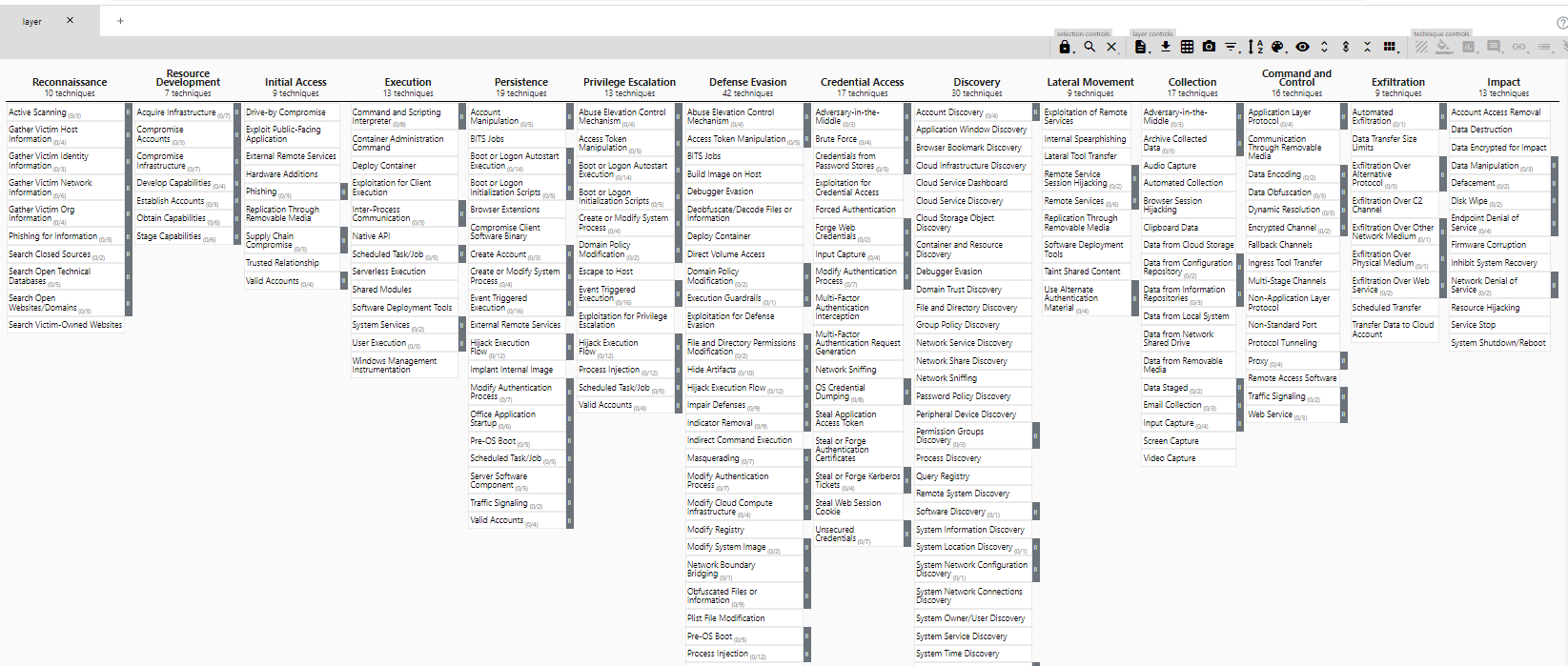
Es la herramienta de Mitre para poder “pintar” de forma online la matriz Mitre de un determinado cliente. Se puede pintar de forma “manual”, pero nosotros usaremos varios script para obtener un archivo .json y poder subirlo directamente a la siguiente dirección y obtener los heatmaps correspondientes:

[**https://mitre-attack.github.io/attack-navigator/**](https://mitre-attack.github.io/attack-navigator/)

Los scripts a usar son los siguientes:

[**https://github.com/rabobank-cdc/DeTTECT**](https://github.com/rabobank-cdc/DeTTECT)

[**https://github.com/gonzalomarcos/Personal/tree/master/EDRs**](https://github.com/gonzalomarcos/Personal/tree/master/EDRs)



1. Obtención heatmaps

La obtencion se realizará a partir de CSV generado previamente con las TTP y el score asigando. Para ello, se deberá tener instlado python en el ordenador. SE obtendrá el script del siguiente GitHub:

<https://github.com/gonzalomarcos/Personal/blob/master/EDRs/MITREEDR.py>

Una vez obtenido el script, se cambiará la linea 9 y 10 por el nombre del archivo que vamos a importar (el csv) y el nombre con el que queramos que nos saque el yaml.

Una vez obtenido el archivo yaml correspondiente, el siguiente paso es instalar y usar la herramienta de Rabobank, denominada: rabobank-cdc/DeTTECT.

<https://github.com/rabobank-cdc/DeTTECT>

Para ello, abrá que descargarse la ultima versión. Una vez descargada, descomprimirla donde el usuario desee. Una vez descompirimido, ingresaremos en la carpeta **“MITRE\_RABOBANK/DeTTECT-1.7.0/sample-data**/” y pegaremos el yaml obtenido previamente.

Seguidamente, abriremos un terminal y ejecutaremos lo siguiente:

**python dettect.py d -ft sample-data/techniques-administration-endpoints.yaml -l**

Con ello obtendremos el heatmap de lo que nuestro cliente si tiene totalmente o parcialmente cubierto en color verde asi como lo que no tiene cubierto en color blanco.

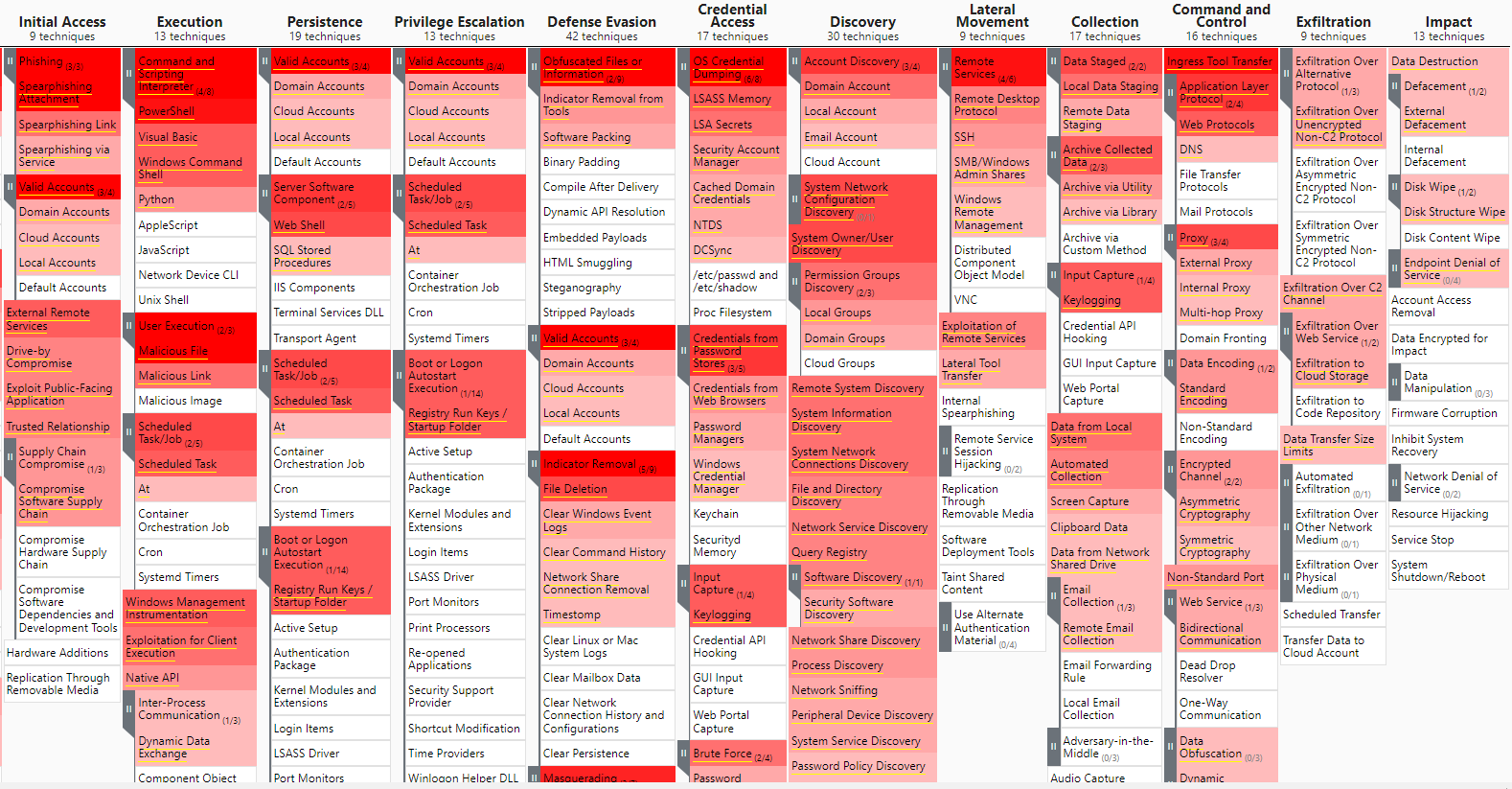
Se obtendrá algo parecido al mapa de calor inferior.



Para obtener el heatmap de los grupos atacantes que pueden afectar a dicho cliente, será necesario ejecutar el siguente comando:

**python dettect.py g -g sample-data/groups.yaml**

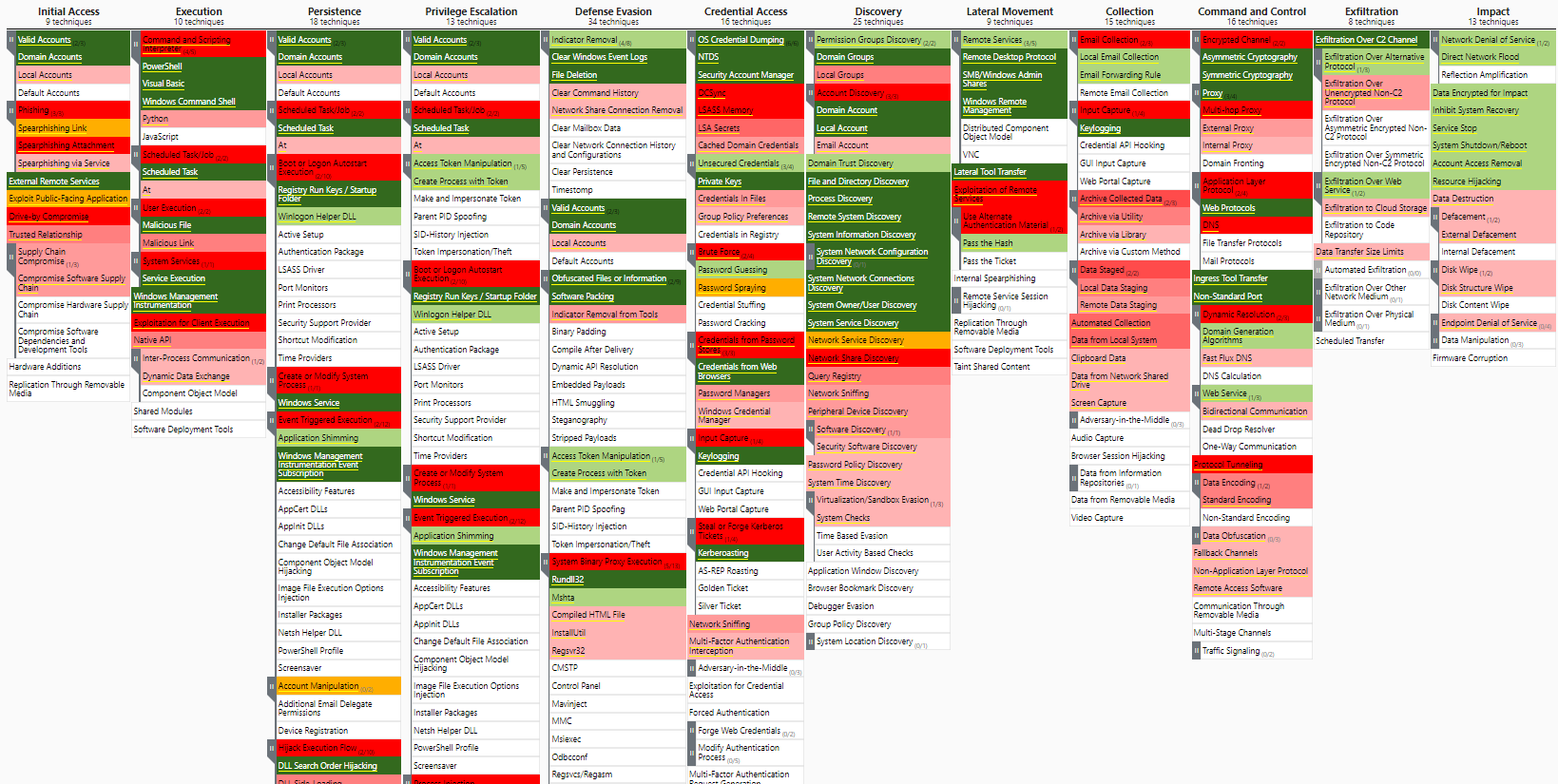
Deberia mostrarse algo similar a la imagen inferior.

****

Por ultimo, quedaria obtener el GAP (como el de la imagen inferior), el cual es el heatmap que combina lo que el cliente tiene cubierto, con lo que tiene parcialmente o sin cubrir. Para ello, necesitará el yaml de los grupos atacantes de ese cliente en concreto, Si el cliente pertenece al sector financiero, se usará el yaml correspondiente a los atacantes del grupo financiero. Por ello, habrá que incorporar ese yaml a la ruta indicada anteriormente: “MITRE\_RABOBANK/DeTTECT-1.7.0/sample-data/” . Y posteriormente se ejecutará el sigueinte comando:

**python dettect.py g -g sample-data/groups.yaml -o sample-data/techniques-administration-endpoints.yaml -t detection**

Para comprender los colores obtenidos, observe el apartado 7.



1. Score estandarizado

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| COLORES |  |  |  |  |  |  |  |
| DETECCIÓN | \*No cubierto | \*Muy cubierto | \*Muy cubierto | \*Parcialmente cubierto | \*Parcialmente cubierto | \*No cubierto | \*No cubierto |
| GRUPOS | \*No usado | \*Poco usado | \*Muy usado | \*Poco usado | \*Muy usado | \*Poco usado | \*Muy usado |
| SCORE | - | SCORE(4-5) | SCORE(4-5) | SCORE(2-3) | SCORE(2-3) | SCORE(0-1) | SCORE(0-1) |