ISMAEL VALENZUELA - @ABOUTSECURITY

MODELADO PRÁCTICO DE AMENAZAS Y DEFENSAS BLUE TEAM CON MITRE ATT&CK

Fundador de
G2 Security en 2000

Ingeniero Principal
Senior en McAfee

Autor e Instructor del
Instituto SANS

@aboutsecurity


MITRE qué??

PIENSA EN ROJO, ACTUA EN AZUL

- Un ataque (red team) que no resulta en la mejora del programa de seguridad no sirve para nada.
- La defensa (blue team) que no está priorizada por las amenazas y el impacto, no es efectiva.
- Es todo gestión de riesgos…
- **MITRE ATT&CK** te permite priorizar de manera práctica en qué enfocar tu defensa, mediante el conocimiento del enemigo.

¿Dónde comenzamos?

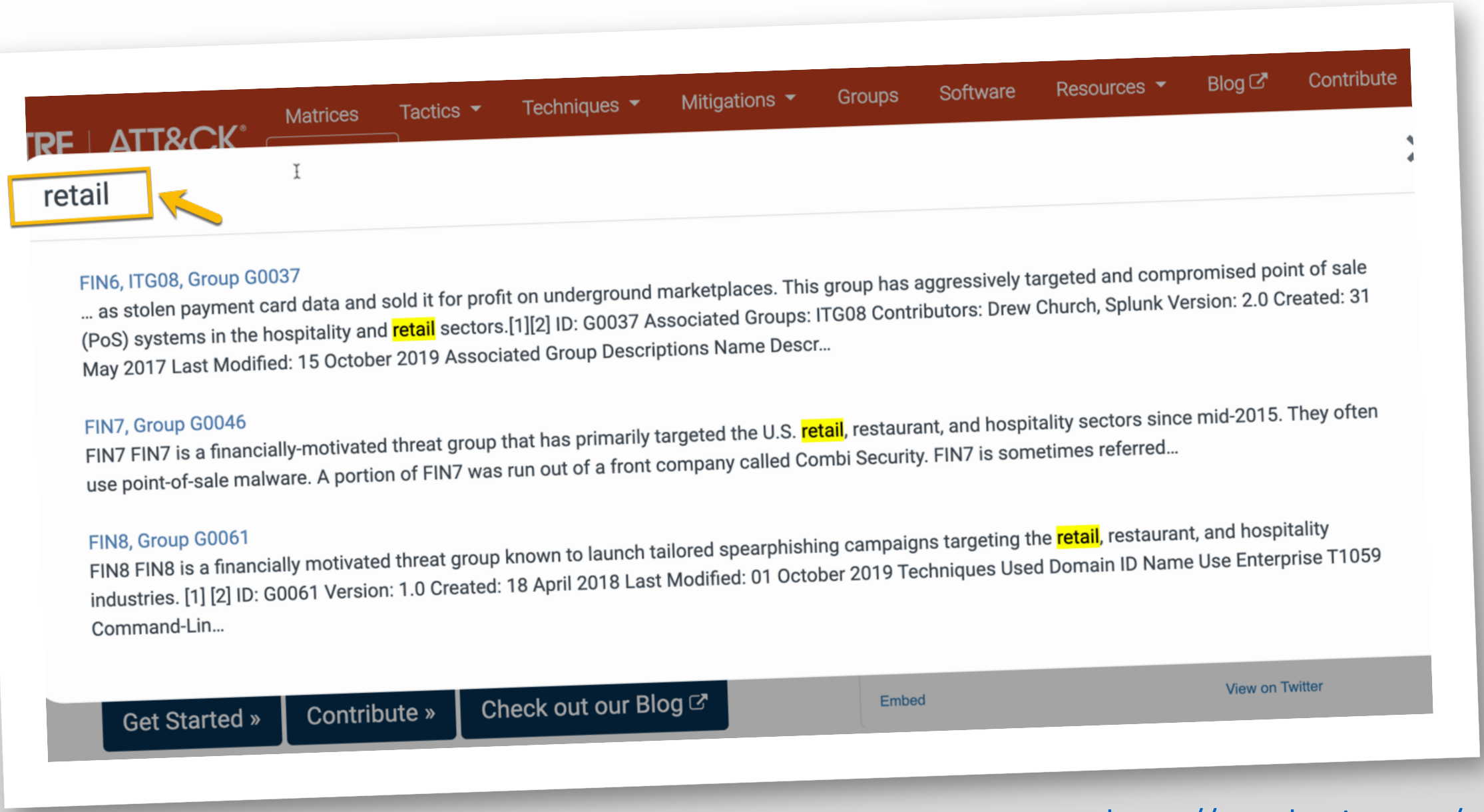
CASO DE USO: **HACME CATS**

Negocio: venta de comida para gatos online

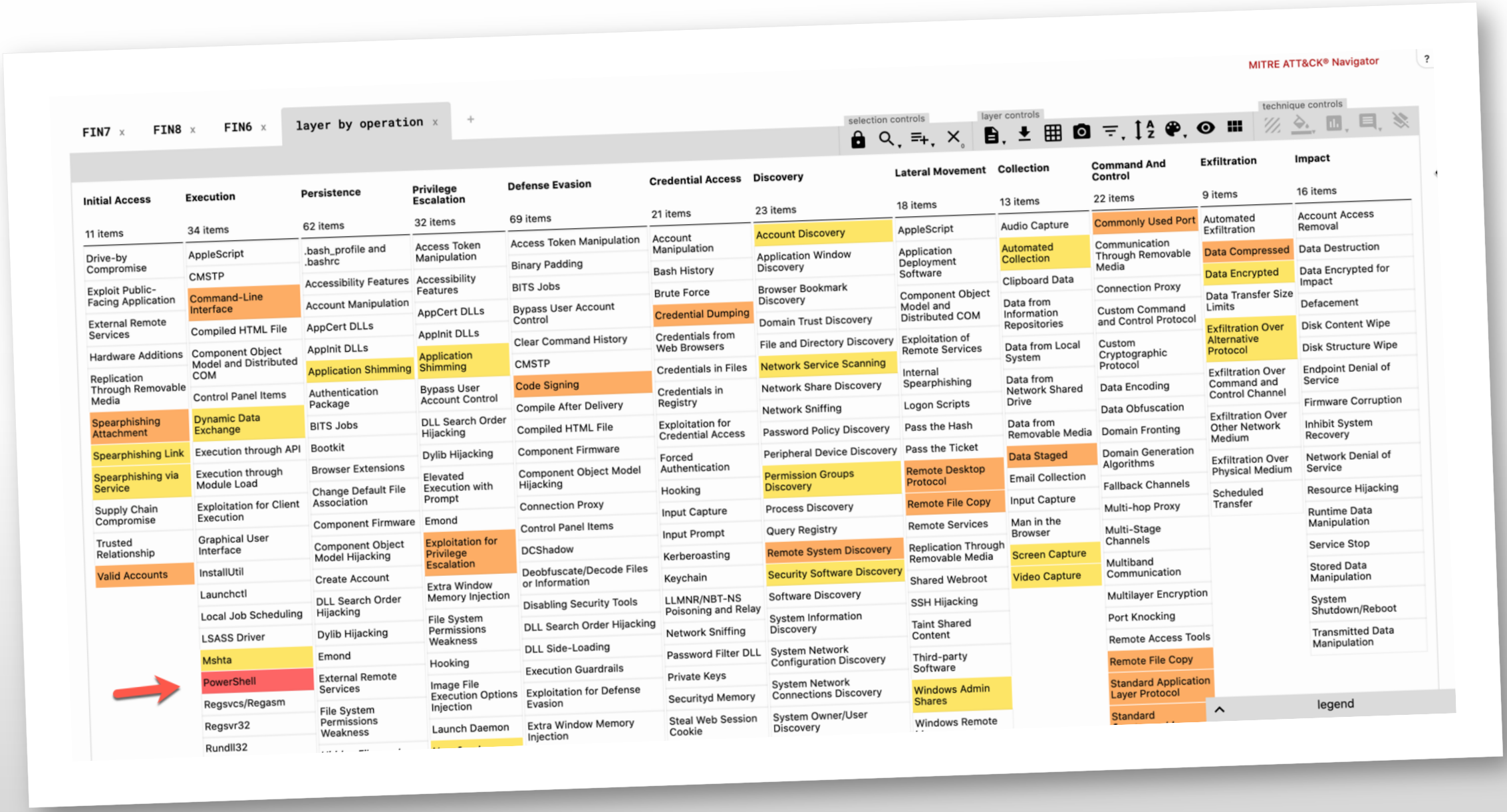
Amenaza: FIN-Dogs (súper APT)

Herramientas:

- Página de MITRE ATT&CK
  - https://attack.mitre.org/
- ATT&CK Navigator
  - https://mitre-attack.github.io/attack-navigator/



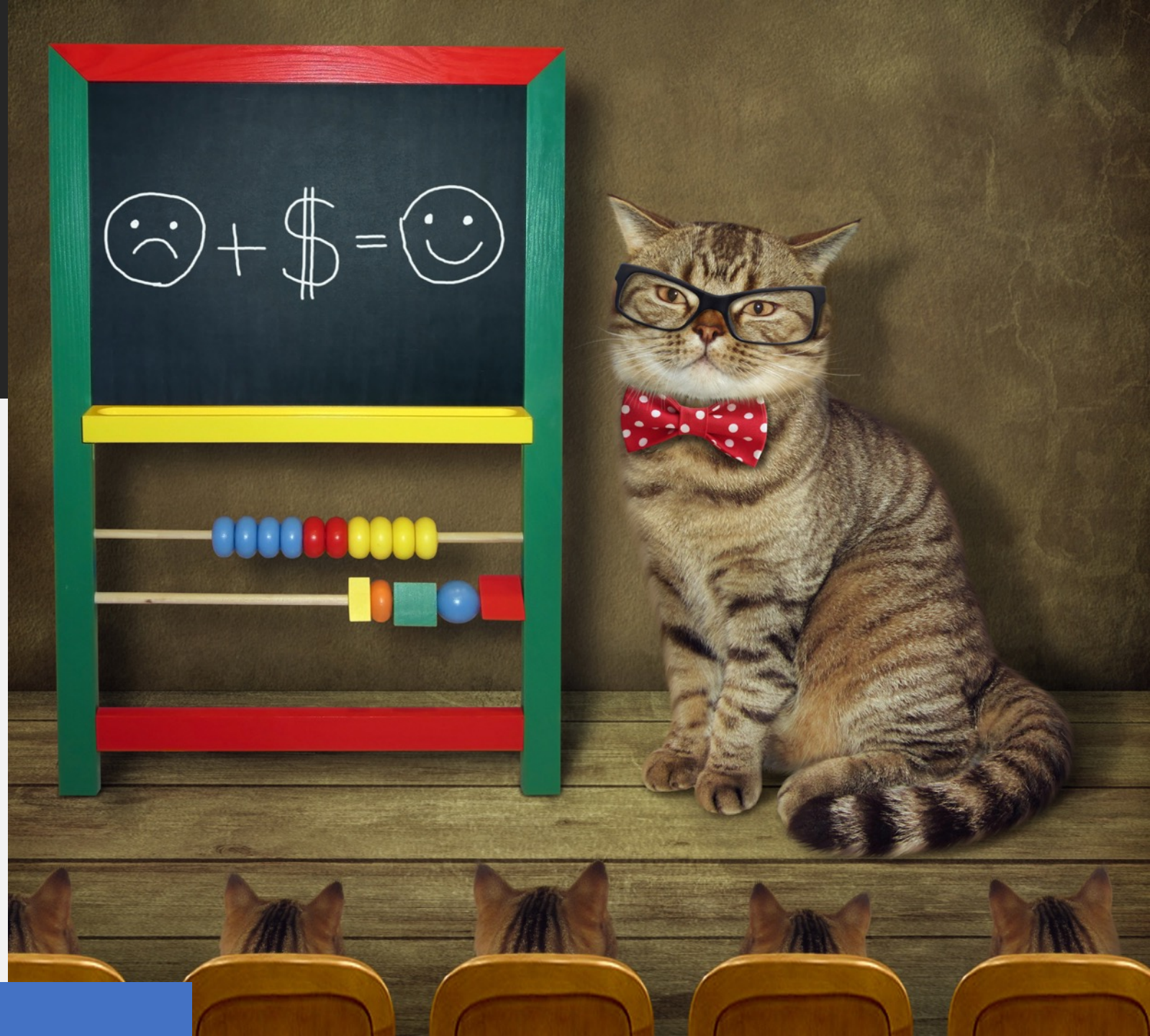
https://attack.mitre.org/



https://mitre-attack.github.io/attack-navigator/enterprise/#

Juguemos con algunas analíticas

- ATT&CK scripts: https://github.com/mitre-attack/attack-scripts
- Jupyter notebook: https://mybinder.org/v2/gh/mitre-attack/attack-scripts/master
- ATT&CK Python client: https://github.com/hunters-forge/ATTACK-Python-Client



Data Source Investigation

Let's use the ATT&CK Python Client to manually examine the techniques, list the data sources, and build a heatmap out of our selected sources.

If you're looking for less development or a more in-depth and finely-grained dive, check out:

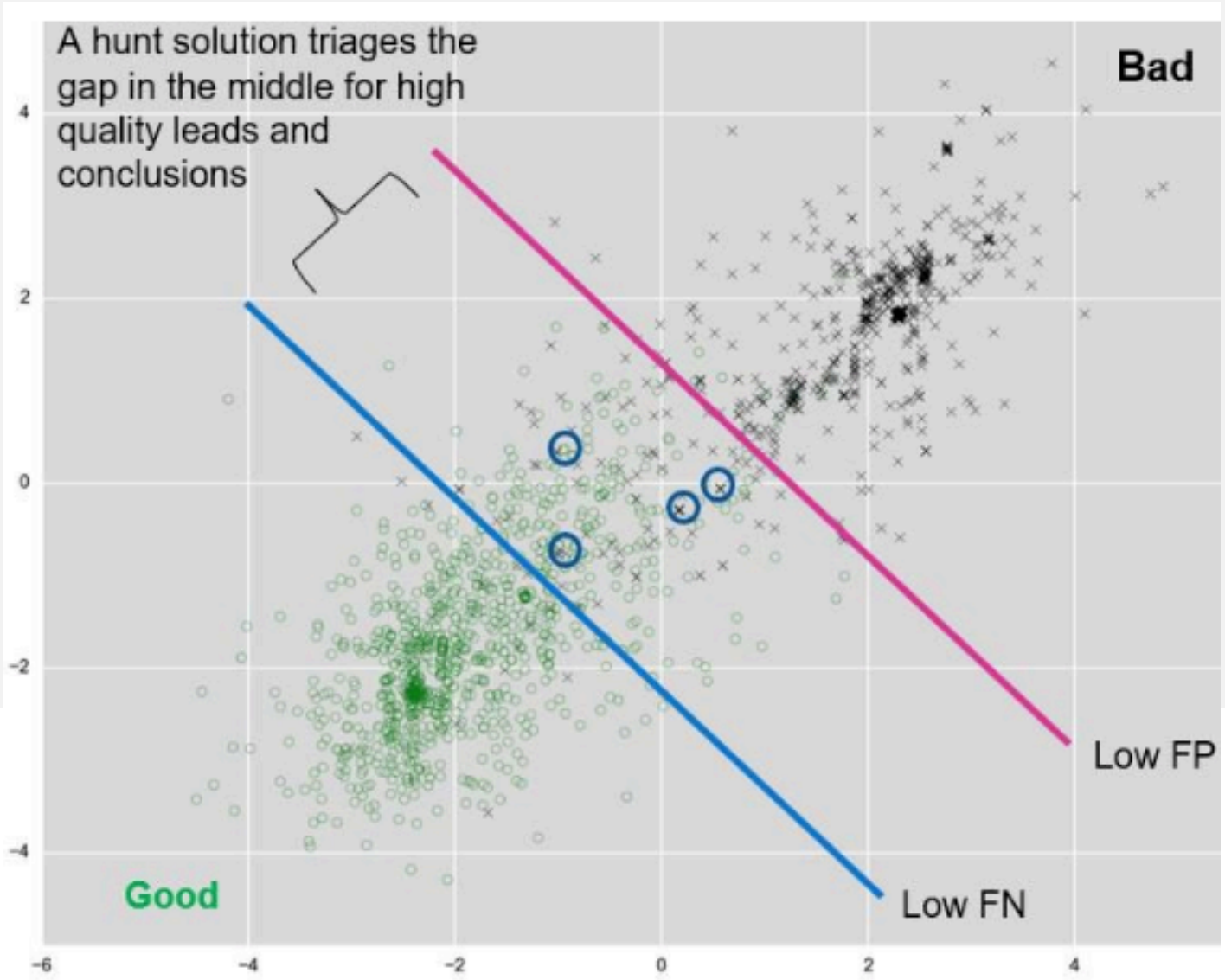
- DeTTACK
- AttackDatamap

Consider: What have you used to track data sources? What has worked well, and what has not worked so well?

In [ ]:
```
# Import the packages we'll need

# Some basic python and jupyter stuff
from collections import defaultdict
import json
from IPython.display import FileLink, FileLinks

# Visualization and data libraries
import altair as alt
import pandas as pd

# ATT&CK Python Client, by @HuntersForge (https://github.com/hunters-forge/ATTACK-Python-Client)
from attackcti import attack_client

# Because this is in Jupyter notebooks we need to enable that renderer for the altair charts to work
alt.renderers.enable('notebook')
```

Get the ATT&CK Enterprise techniques using the client library

In [ ]:
```
client = attack_client()
all_techniques = client.get_enterprise()['techniques'] # Note - this takes a few seconds to download and parse
```

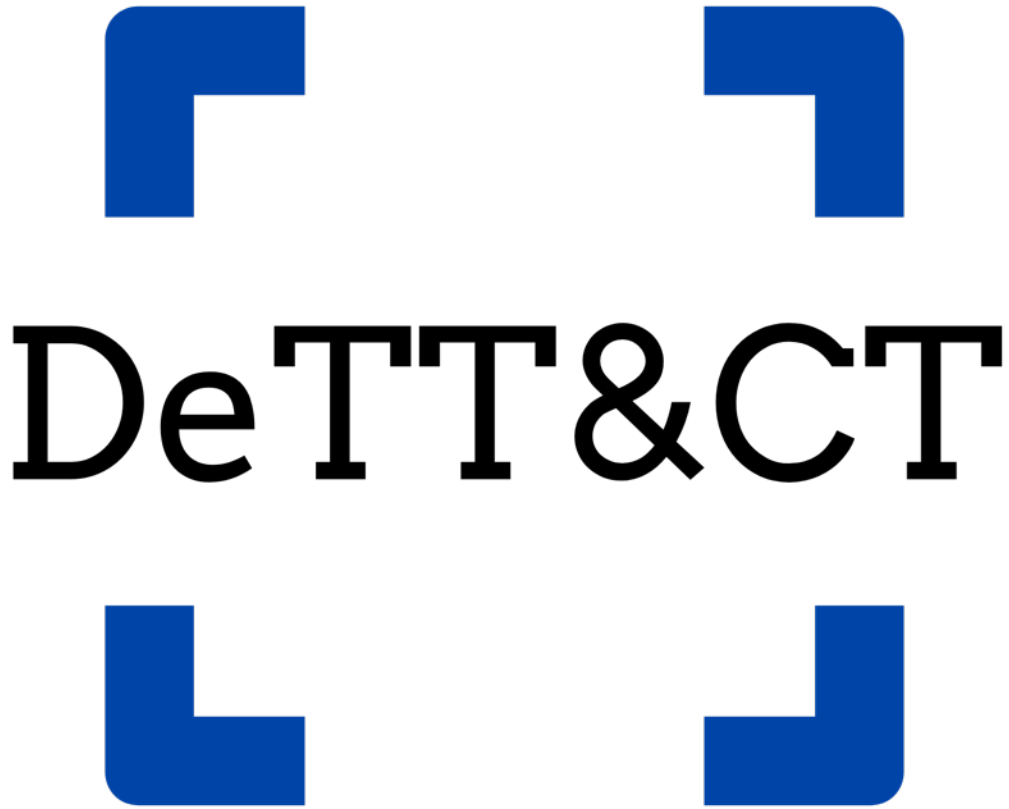


Visibilidad vs Detección

La mayoria de productos de detección no son adecuados para threat hunting.

- Prevención y Detección -- Pocos FPs
- Visibiliidad y Hunting – Pocos FNs

https://deltarisk.com/blog/why-most-real-time-defensive-solutions-are-poor-threat-hunting-solutions/



- Framework para administrar, evaluar y comparar la calidad de:
  - Data sources
  - Visibilidad
  - Detección
  - Threat actors

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

Data Sources

- https://github.com/rabobank-cdc/DeTTECT/wiki/Data-sources
- Casi 60 fuentes de datos aplicables a distintas plataformas

Home > Techniques > Enterprise > Standard Application Layer Protocol

Standard Application Layer Protocol

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

https://attack.mitre.org/techniques/T1071/

ID: T1071

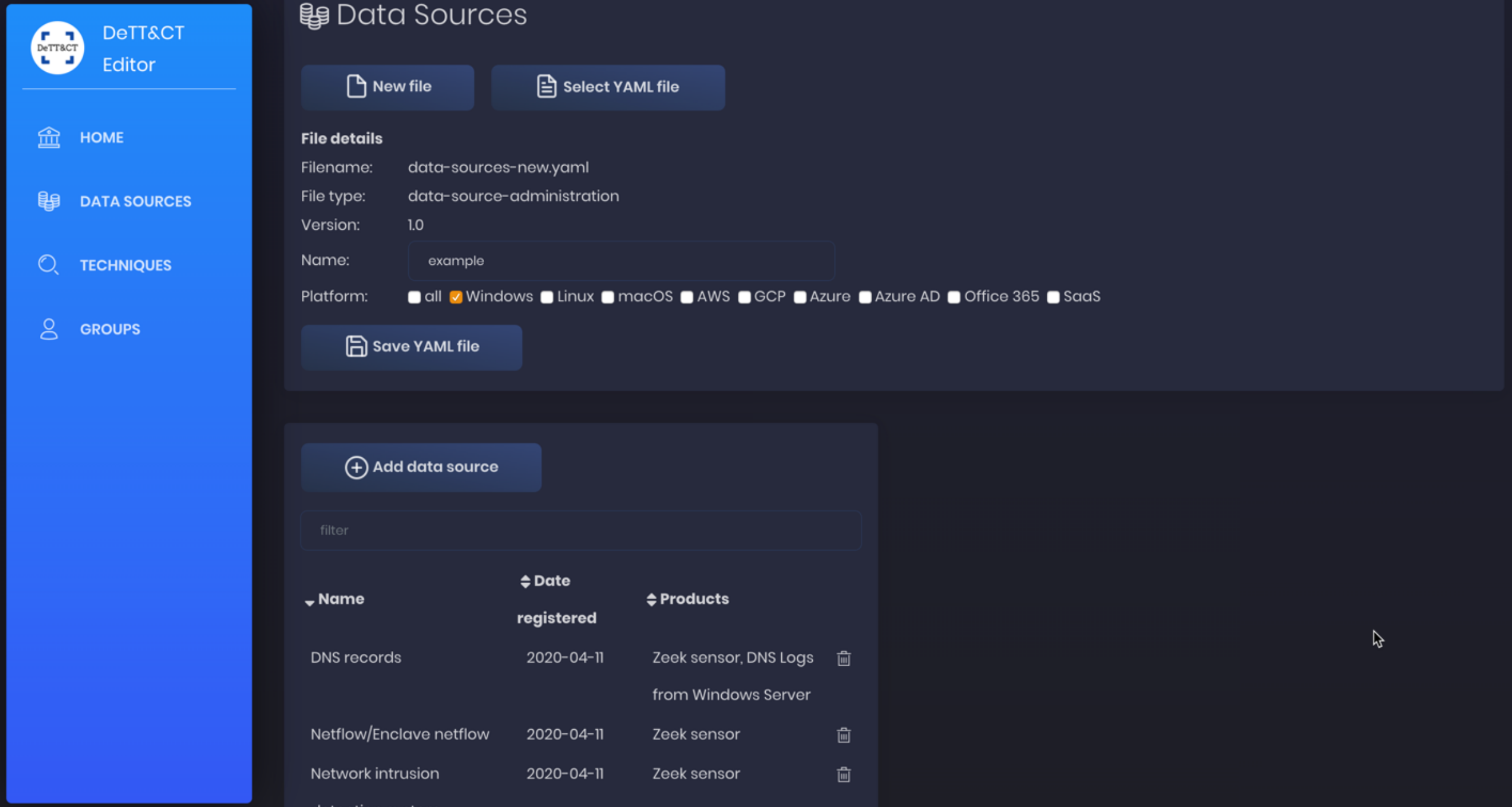
Tactic: Command And Control

Platform: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

Version: 1.0


DeTT&CT Editor
HOME
DATA SOURCES
TECHNIQUES
GROUPS
Data Sources
New file
Select YAML file
File details
Filename: data-sources-new.yaml
File type: data-source-administration
Version: 1.0
Name: example
Platform: all Windows Linux macOS AWS GCP Azure Azure AD Office 365 SaaS
Save YAML file
Add data source
filter
Name
Date registered
Products
DNS records 2020-04-11 Zeek sensor, DNS Logs from Windows Server
Netflow/Enclave netflow 2020-04-11 Zeek sensor
Network intrusion detection system 2020-04-11 Zeek sensor

MITRE ATT&CK® Navigator

FIN6 x | FIN7 x | FIN8 x | Data sources example x | Visibility example x | Detections example x | FIN6+FIN7+FIN8 - Attack - Windows x | +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Mshta	Create Account	New Service	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Taint Shared Content	Video Capture	Multiband Communication		Service Stop
	PowerShell	DLL Search Order Hijacking	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Third-party Software		Multilayer Encryption		Stored Data Manipulation
	Regsvcs/Regasm	External Remote Services	Path Interception	Disabling Security Tools	Password Filter DLL	Security Software Discovery	Windows Admin Shares		Remote Access Tools		System Shutdown/Reboot
	Regsvr32	File System Permissions Weakness	Port Monitors	DLL Search Order Hijacking	Private Keys	Software Discovery	Windows Remote Management		Remote File Copy		Transmitted Data Manipulation
	Rundll32	Hidden Files and Directories		DLL Side-Loading	Steal Web Session Cookie	System Information Discovery			Standard Application Layer Protocol		
	Scheduled Task	Hooking		Execution Guardrails	Two-Factor Authentication	System Network Configuration Discovery					
	Scripting			Exploitation for Defense Evasion		System Network					
	Service Execution			Extra Window Memory Injection							
				File and Directory							

Ajustar visibilidad y detección

Visibilidad

- https://github.com/rabobank-cdc/DeTTECT/wiki/Visibility-coverage
- Genera un fichero JSON con la cobertura de visibiliidad en base a la plantilla de administración de técnicas: **python dettect.py v -ft sample-data/techniques-administration-endpoints.yaml -fd sample-data/data-sources-endpoints.yaml -l**
- La leyenda indica el tipo de visibilidad en base al input proporcionado.

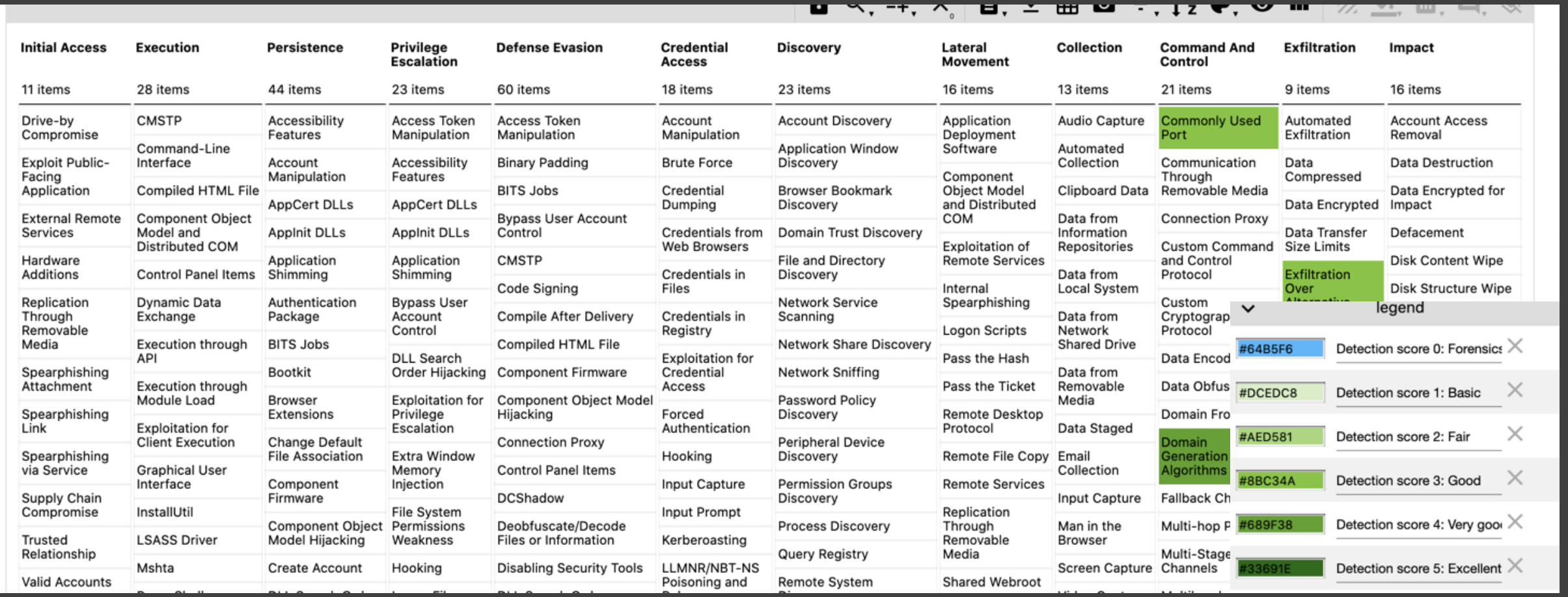
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation		Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fron		Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms		Inhibit System Recovery
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Cha		
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop P		
	LSASS Driver	Component Object Model Hijacking	Image File	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		
	Mshta	Create Account		DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry		Video Capture	Multiband		
	PowerShell	DLL Search Order		Deobfuscate/Decode Files or Information		Remote System Discovery					
				Disabling Security Tools							
				DLL Search Order							

legend

#BBDEFB	Visibility score 1: Minimal
#64B5F6	Visibility score 2: Medium
#1976D2	Visibility score 3: Good
#0D47A1	Visibility score 4: Excellent

Detección

- https://github.com/rabobank-cdc/DeTTECT/wiki/Detection-coverage
- Genera un fichero JSON con la cobertura de detecciones en base a la plantilla de administración de técnicas: **python dettect.py d -ft sample-data/techniques-administration-endpoints.yaml -l**
- La leyenda indica la calidad de las detecciones en base al input proporcionado.



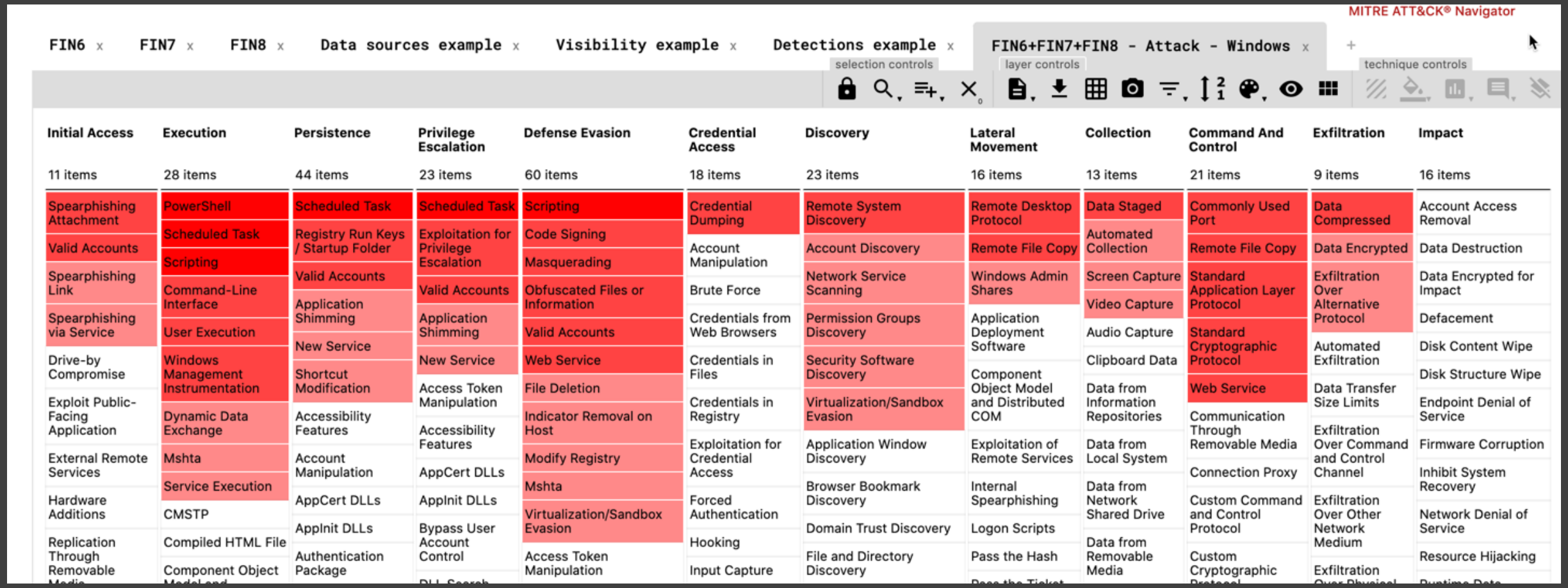
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptograp Protocol	Exfiltration Over Alternative	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encod		Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfus		
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fro		
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms		
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Ch		
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop P		
	LSASS Driver	Component Object Model Hijacking		Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		
	Mshta	Create Account		DCShadow	LLMNR/NBT-NS Poisoning and	Query Registry					
				Deobfuscate/Decode Files or Information		Remote System					
				Disabling Security Tools							

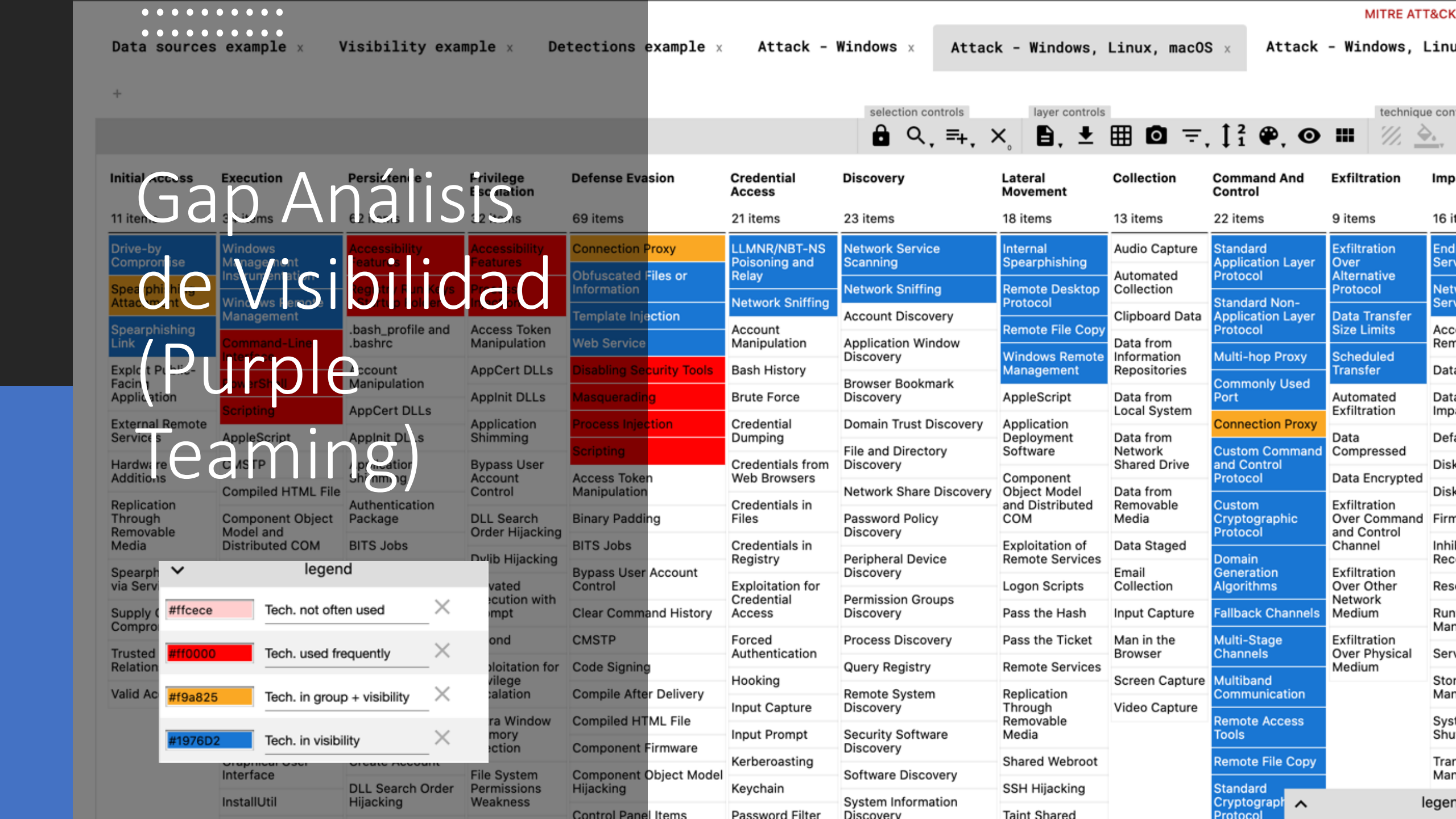
legend

#64B5F6	Detection score 0: Forensics
#DCEDC8	Detection score 1: Basic
#AED581	Detection score 2: Fair
#8BC34A	Detection score 3: Good
#689F38	Detection score 4: Very goo
#33691E	Detection score 5: Excellent

Threat Actors

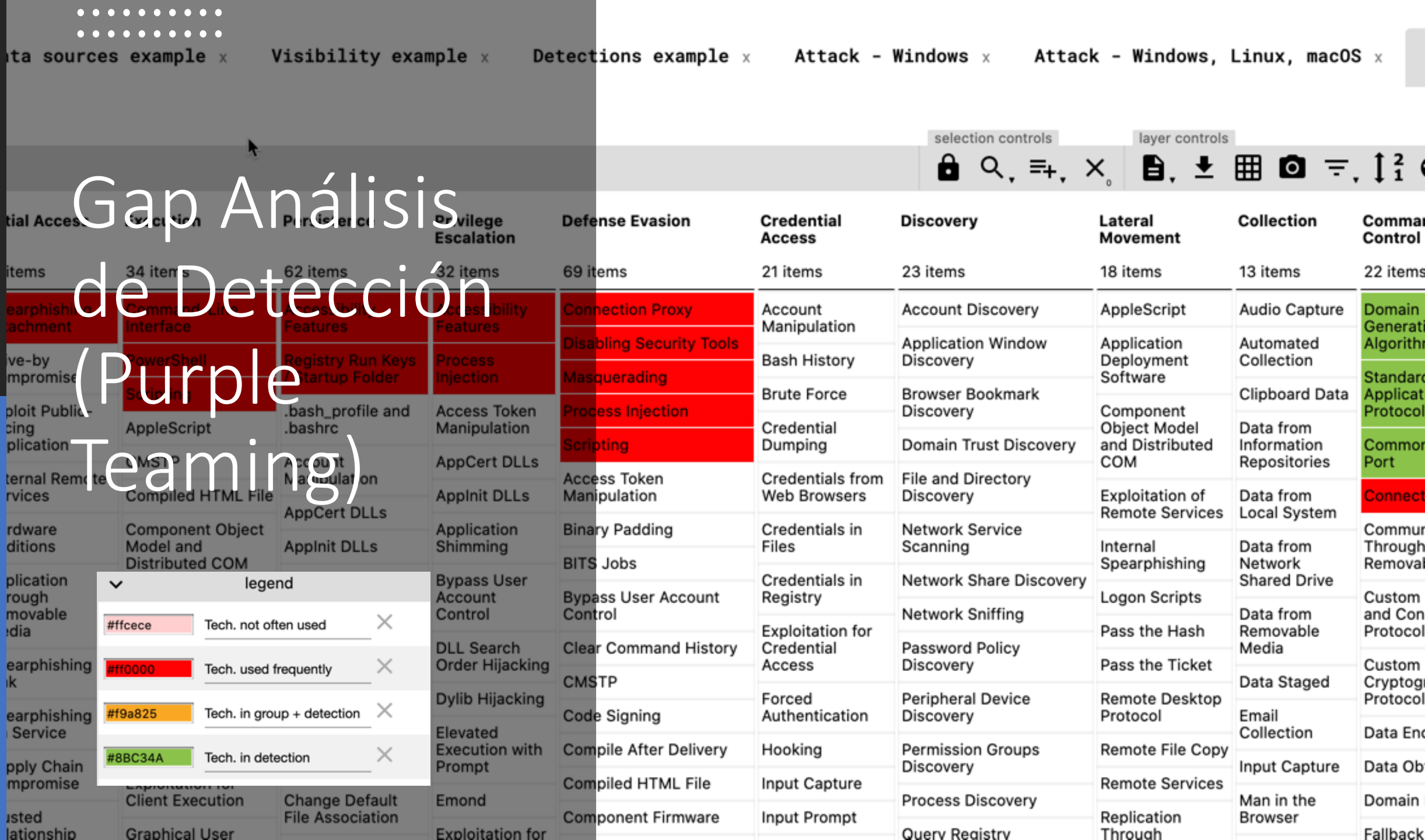
- https://github.com/rabobank-cdc/DeTTECT/wiki/Threat-actor-group-mapping
- Genera un fichero JSON con el heatmap de solo los grupos en los que estamos interesados (FIN6, FIN7, FIN8): python dettect.py g -g 'fin7,fin8,fin6'
- El resultado está ordenado por técnicas más communes (rojo oscuro)





Gap Análisis de Visibilidad (Purple Teaming)

Gap Análisis de Detección (Purple Teaming)



Recursos adicionales

@aboutsecurity

- Thinking Red, Acting Blue - https://www.sans.org/webcasts/defensible-security-architecture-engineering-2-thinking-red-acting-blue-mindset-actions-109710
- Guión de esta charla - https://github.com/aboutsecurity/Talks-and-Presentations/blob/master/c0r0n4con.md
- The Githubification of InfoSec by John Lambert - https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1
- DETT&CT - https://github.com/rabobank-cdc/DeTTECT
- MITRE´s Red Teaming dataset - https://github.com/mitre/brawl-public-game-001