Y qué más da, si …

… son cosas de la E.D.A.D

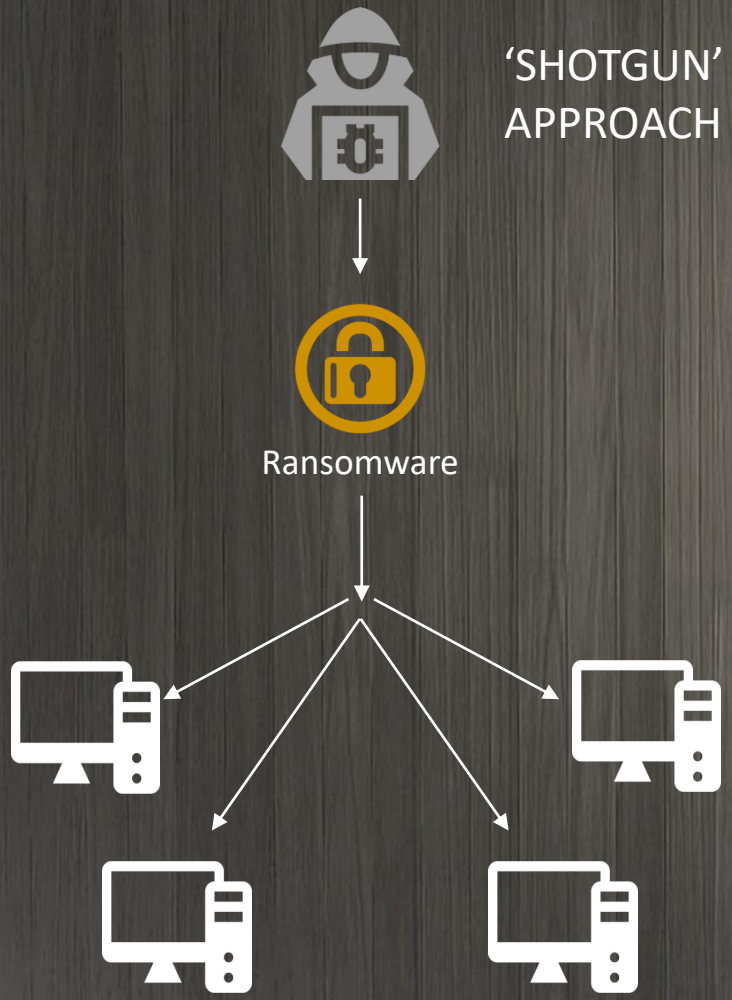
Emilio Rico Ruiz
Grupo TRC

Estrategias de Defensa Activa y Decepcion

Emilio Rico Ruiz
Grupo TRC

DWell Time

(LOS TIEMPOS CAMBIAN)



Ponemon INSTITUTE

IBM Security

287

Average number of days to identify and contain a data breach

Overall, it took an average of 287 days to identify and contain a data breach, **seven days longer** than in the previous report. To put this in perspective, if a breach occurring on January 1 took 287 days to identify and contain, the breach wouldn't be contained until October 14th. The average time to identify and contain varied widely depending on the type of data breach, attack vector, factors such as the use of security AI and automation, and cloud modernization stage.

10%

Increase in average total cost of a breach, 2020-2021

The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years.

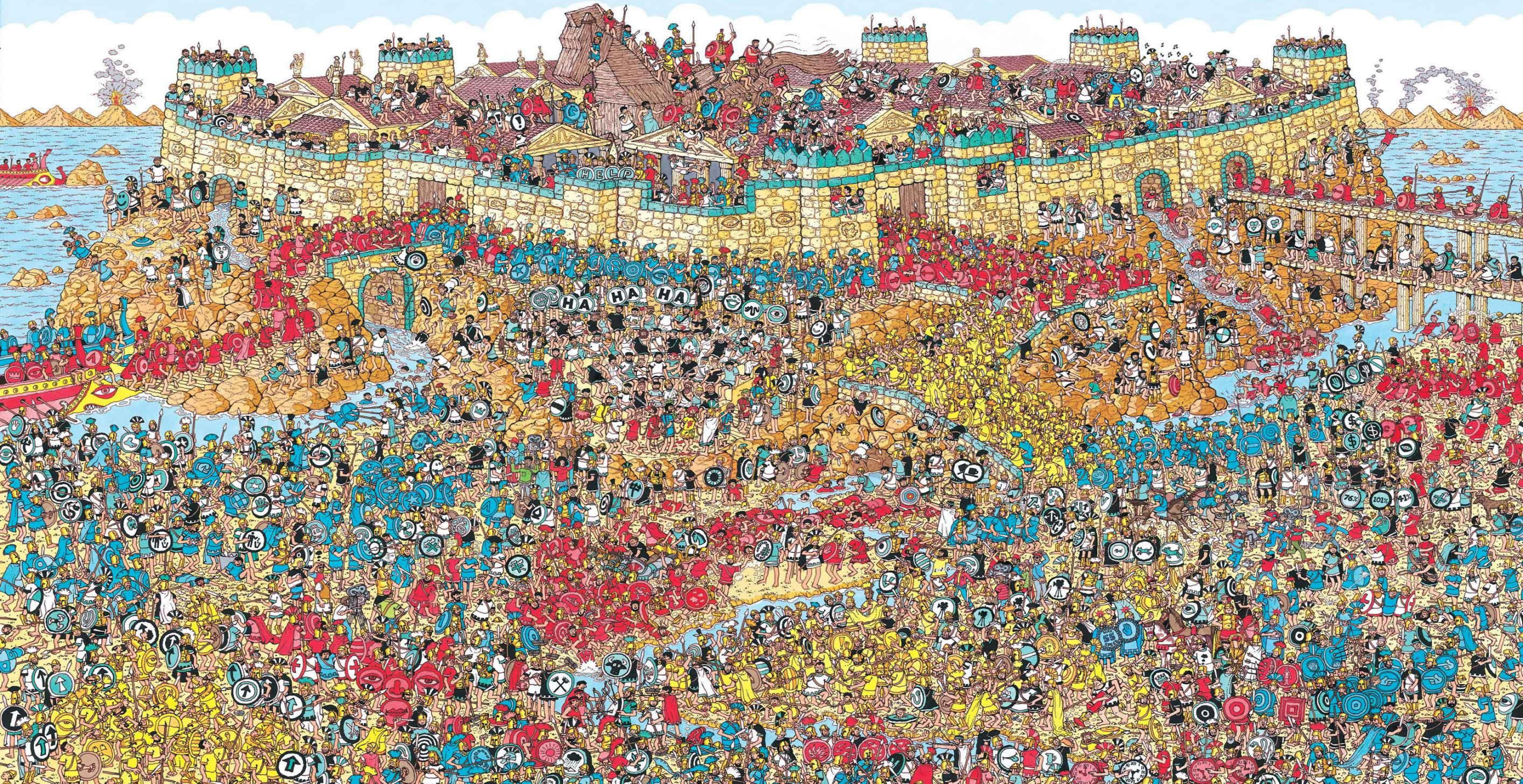
Data breach costs rose from $3.86 million to $4.24 million.

The longer it took to identify and contain, the more costly the breach.

Cost of a Data Breach 2021
https://www.ibm.com/downloads/cas/OJDVQGRY

Entorno
(siempre)
Cambiante

MALA VISIBILIDAD

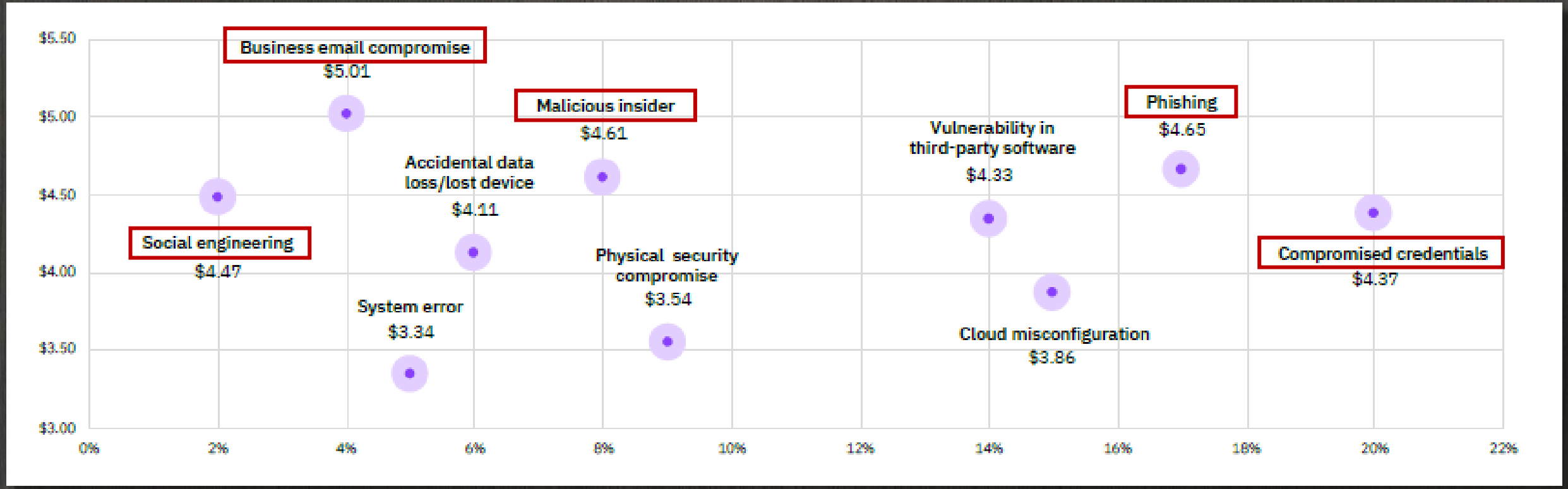


Demasiados falsos positivos

Es este

Average total cost and frequency of data breaches by initial attack vector

60% of attacks **DO NOT** involve malware!



https://md5decrypt.net/en/

15.183.605.161

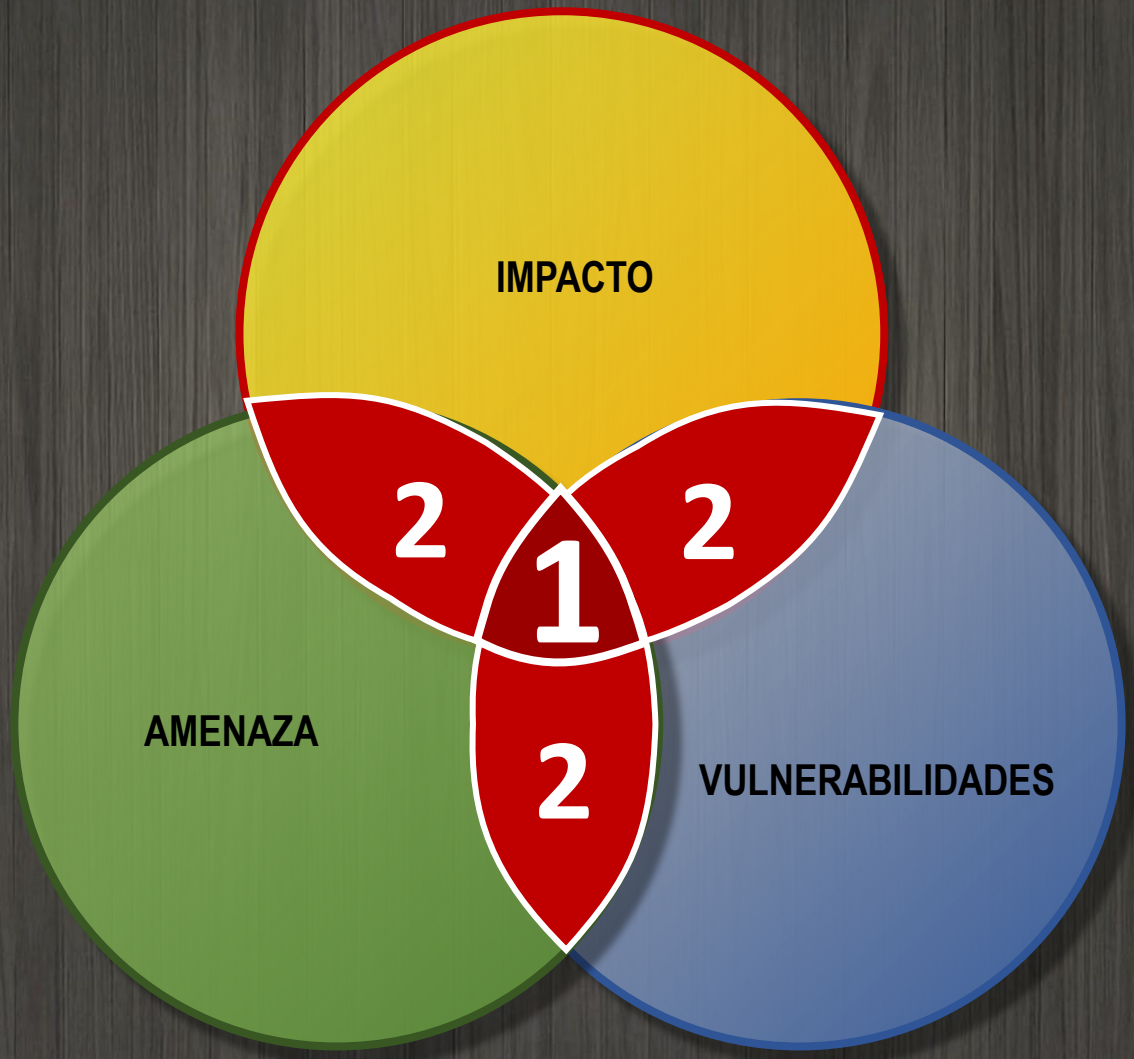
Y si estamos perdiendo …

¿Por qué no cambiamos las reglas del juego?

100%

1 vez

RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



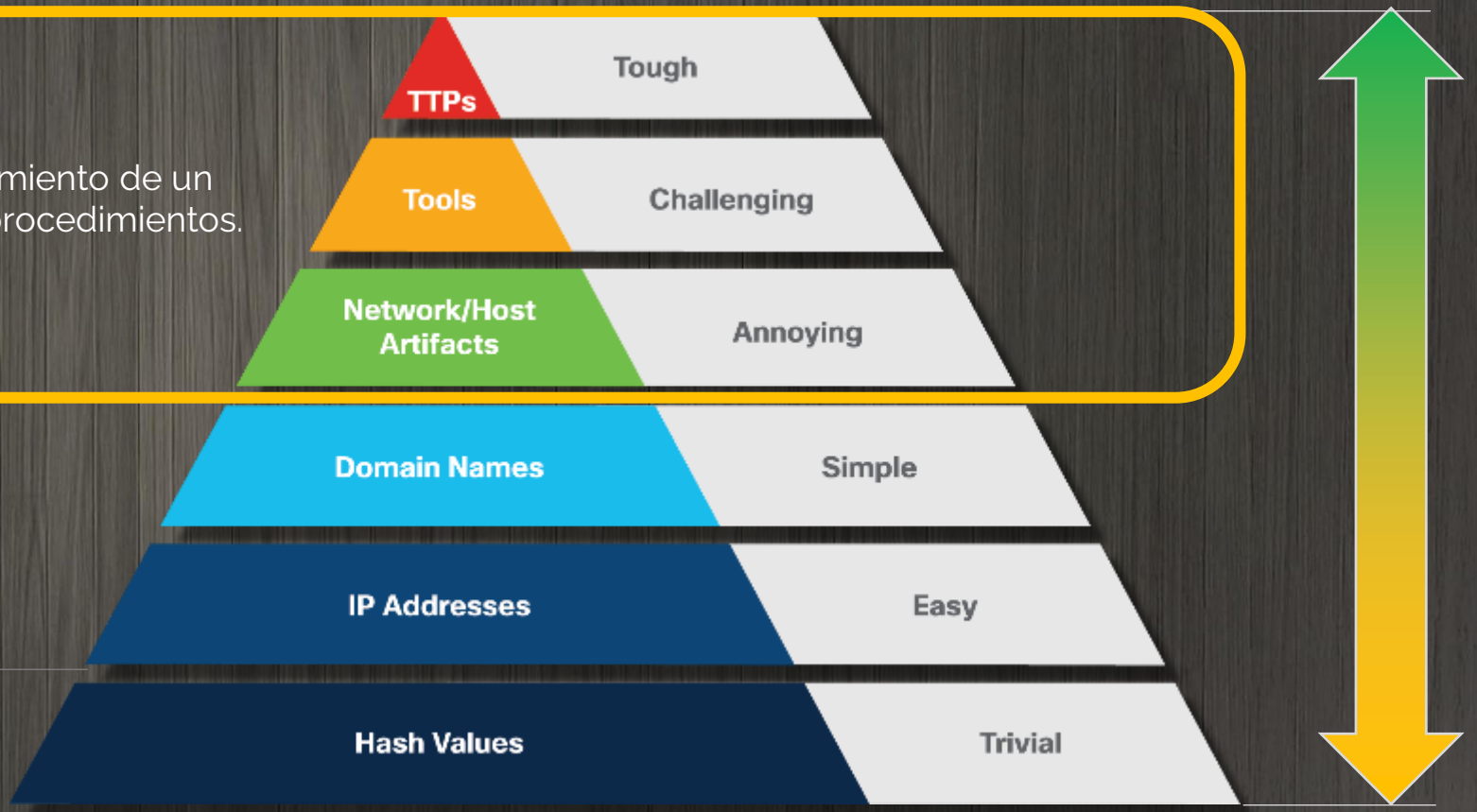
IOC,s

Indicadores conductuales

permiten representar el comportamiento de un atacante, sus tácticas, técnicas y procedimientos.

Indicadores atómicos

Indicadores calculados



The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)

DEFENSA ACTIVA

MAS DIFICIL | MAS LENTO | FORZAR EL ERROR | DESGASTARLO

"Nunca ganes por la fuerza lo que puede ser ganado con el engaño"

Niccolò Machiavelli,
'El discurso'(parafraseado)

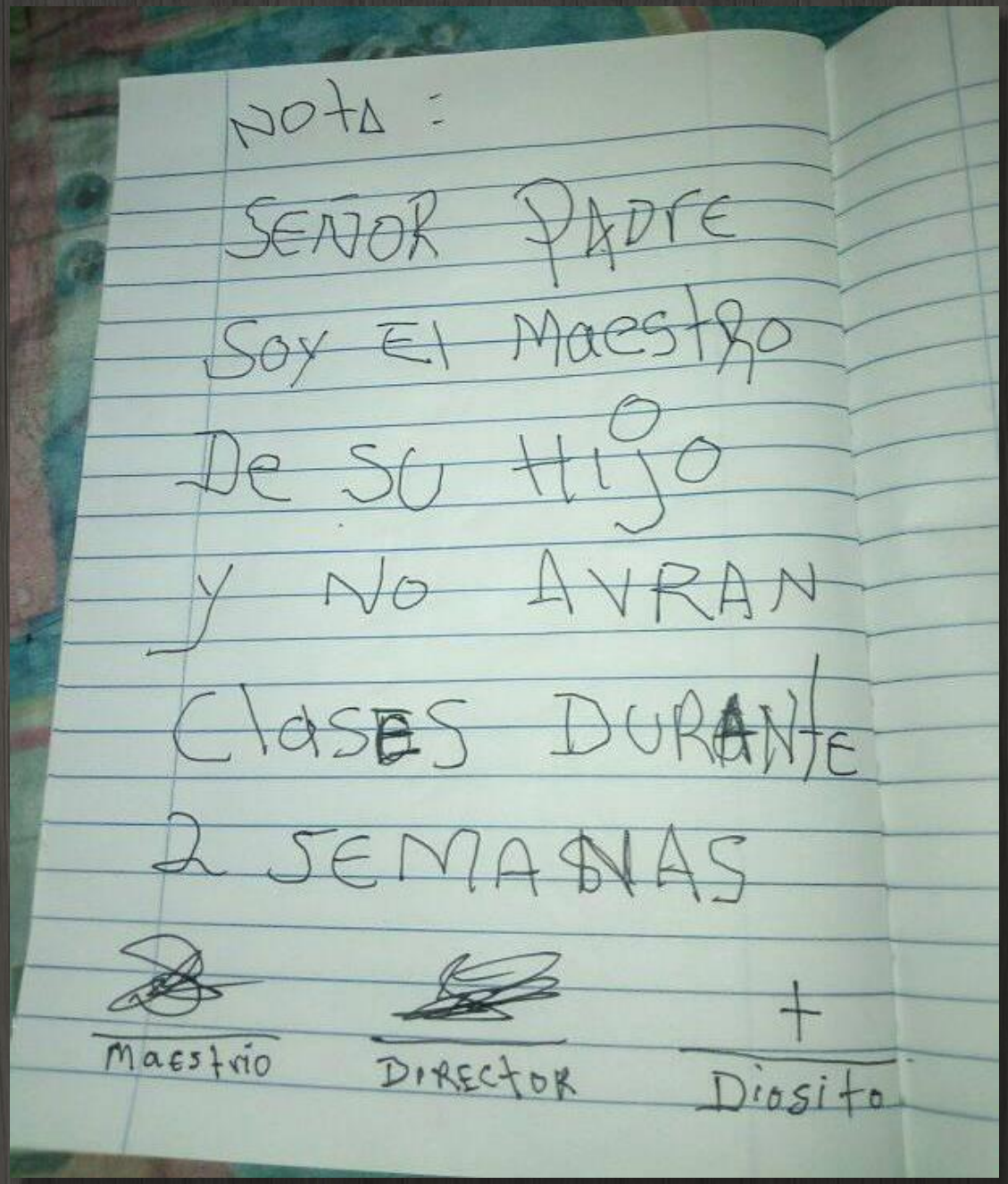
Engaños I - El primer engaño

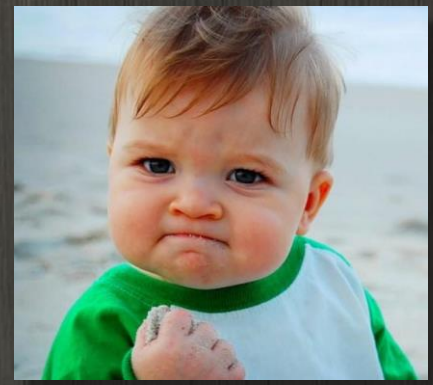
Wenzel Peter. Adán y Eva en el Paraíso Terrenal
Museo Vaticano: Oleo sobre Lienzo

Engaños II: Clásicos de la literatura

Domenico Tiepolo - La procesión del caballo de Troya
National Gallery de Londres: Oleo sobre lienzo

Engaños III
Actitud





Diosito: Facebook

Engaños IV: II WW

https://en.wikipedia.org/wiki/Military_deception

Deception in War - Jon Latimer

MASKIROVKA
маскировка

“Los medios para asegurar las operaciones de combate y las actividades diarias de las fuerzas; una complejidad de medidas, dirigidas a engañar al enemigo con respecto a la presencia y disposición de las fuerzas, su condición, su preparación para el combate y operaciones, y también los planes y objetivos militares del comandante” (1).
Contribuye a la preparación para el combate, el logro de la sorpresa y la consecución de los objetivos

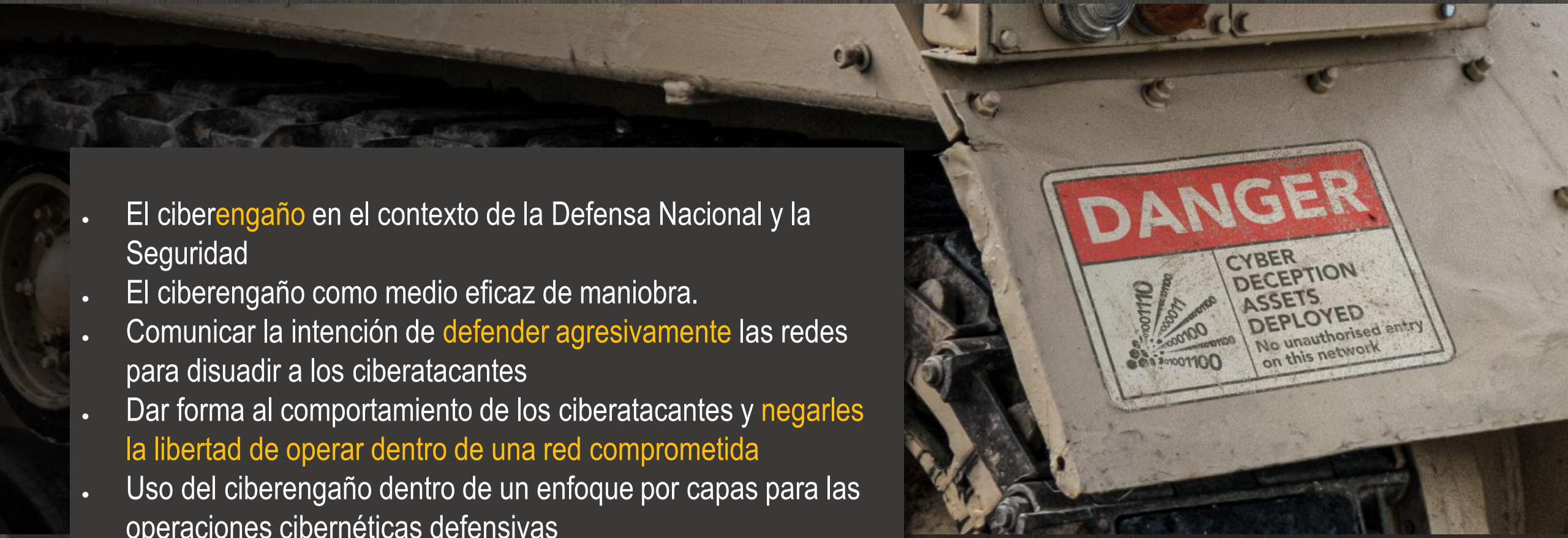
‘ . . . the Soviet armed forces learned to preserve in deep secretiveness the intentions to execute disinformation on a large scale and to deceive the enemy.’

Marshal G. K. Zkukov

(1) Soviet Military Encyclopedia, vol. 5, Moscow, Voyenizdat, 1978, pp. 175–7.

NATIONAL CYBER DECEPTION LABORATORY

Escuela Ciberdefensa- UK MoD
2019



- El ciberengaño en el contexto de la Defensa Nacional y la Seguridad
- El ciberengaño como medio eficaz de maniobra.
- Comunicar la intención de defender agresivamente las redes para disuadir a los ciberatacantes
- Dar forma al comportamiento de los ciberatacantes y negarles la libertad de operar dentro de una red comprometida
- Uso del ciberengaño dentro de un enfoque por capas para las operaciones cibernéticas defensivas

https://www.cyberdeception.org.uk/


DEFENSA ACTIVA
DECEPTION TECHNOLOGIES

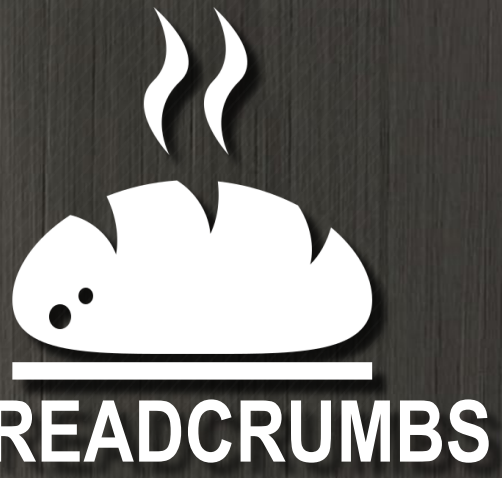
DECEPCION | Cómo funciona?

CAMPAÑA

ESTRATEGIA

HOST & SERVICES

trampas, señuelos …



MIGAS DE PAN

¿INCENTIVOS?

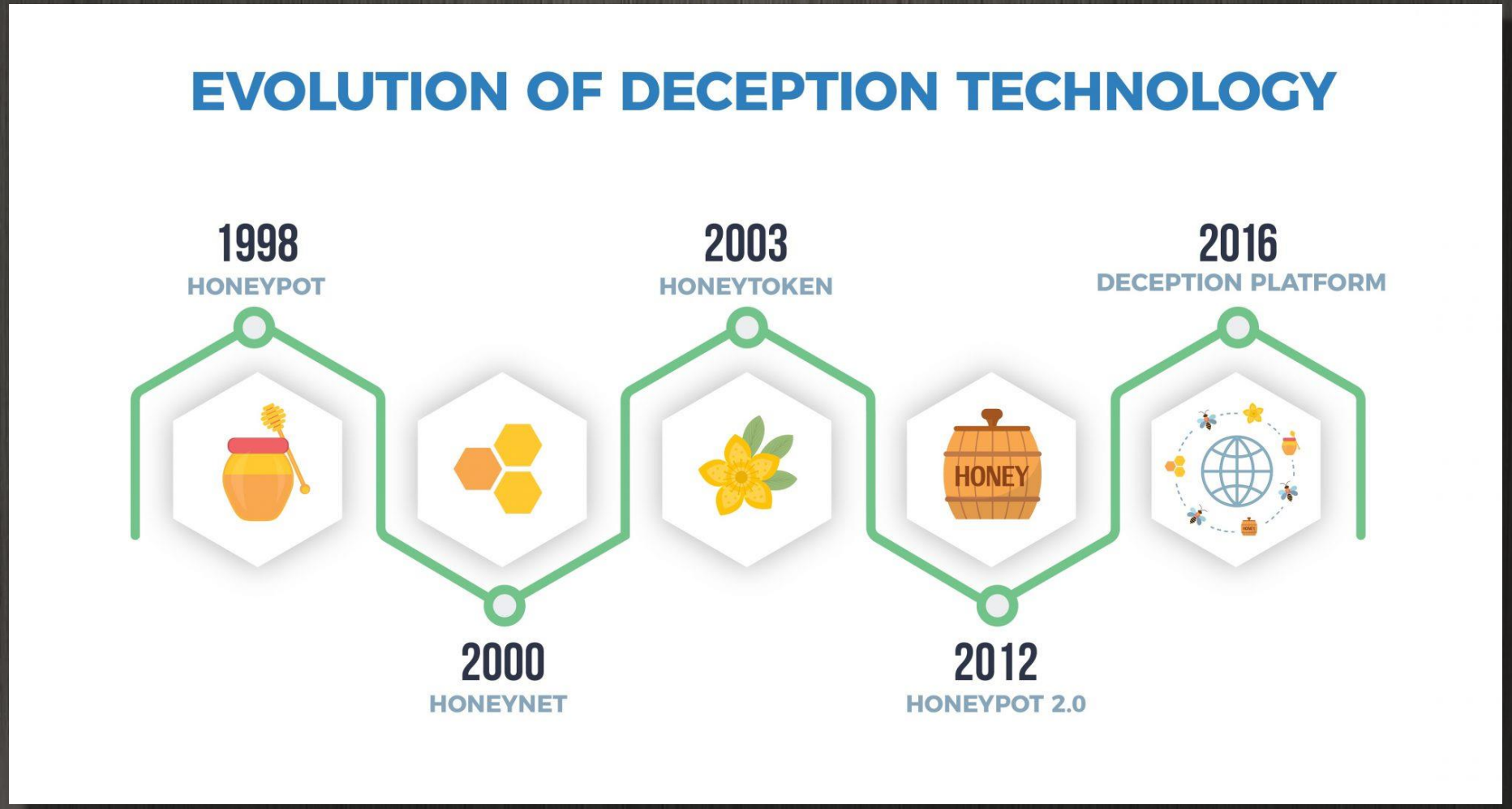
DEFENSA ACTIVA vs HONEY** | No es lo mismo

Honeypots / Honeynets …

- Muy expuestos a Internet
- Atraen los ataques
- Son vulnerables
- Muy centrados en la red
- Poco realistas
- No son escalables

- Útiles en investigación

DEFENSA ACTIVA vs HONEY** | No es lo mismo

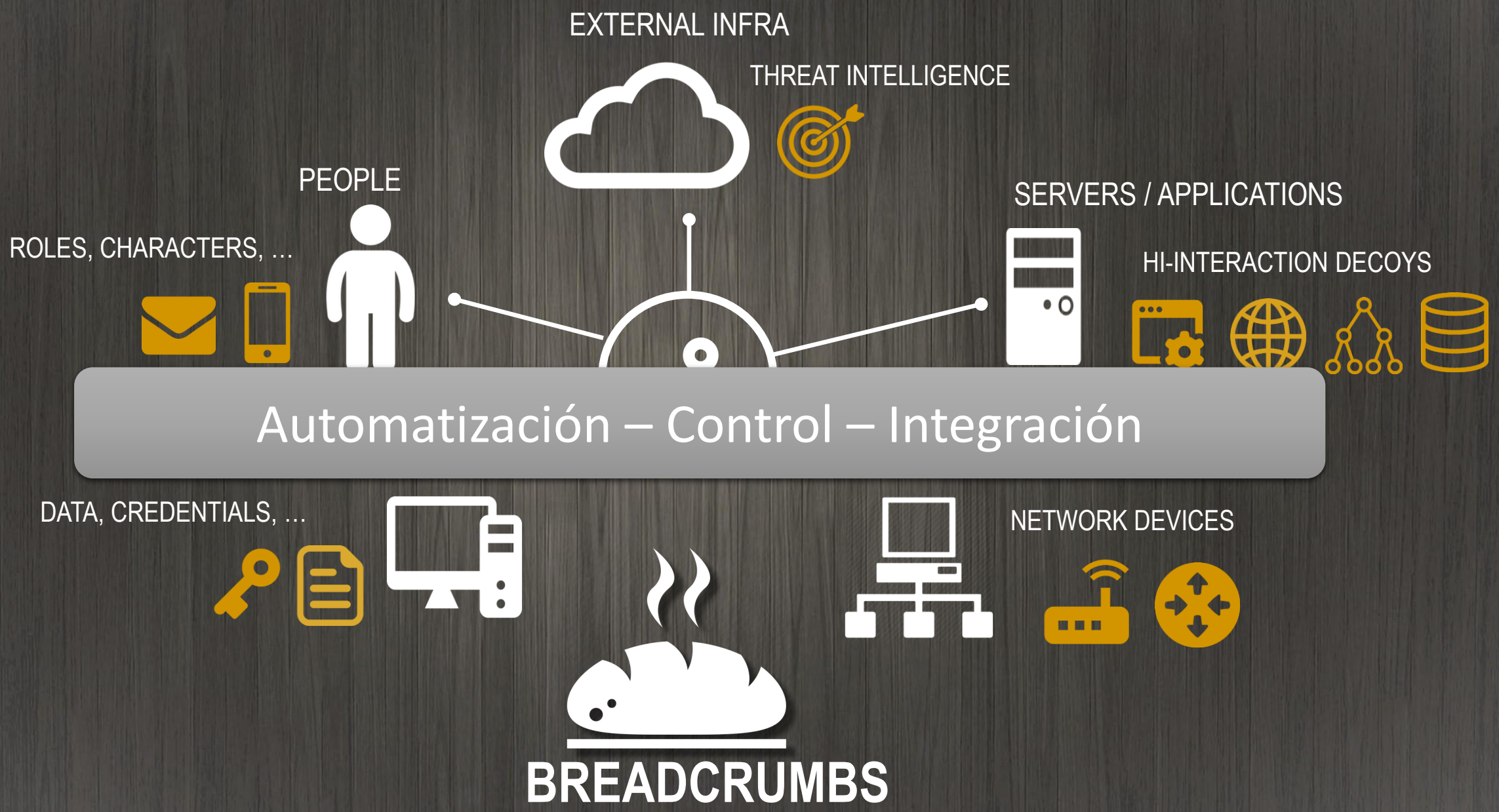


RQ,s

- Debe basarse en datos / servicios.
- Debe cubrir todo el entorno.
- Debe ser flexible (dinámica).
- Debe ser escalable.
- Debe proporcionar automatismos.
- Debe ser inteligente.
- Debe proporcionar inteligencia.
- Debe integrarse con nuestras defensas

- **NO** debe introducir nuevos riesgos.

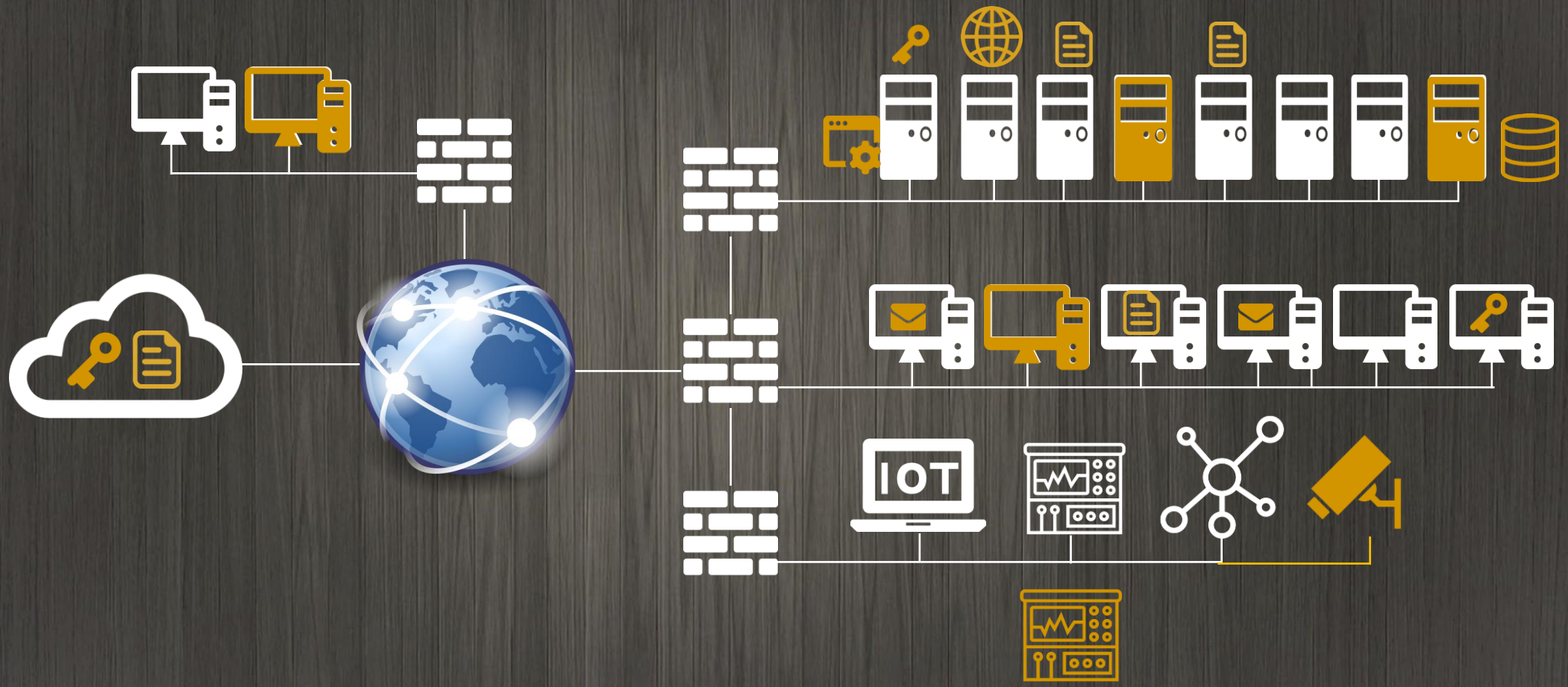
DECEPCION | COMPONENTES



DEFENSA ACTIVA | Soportado por **IA**

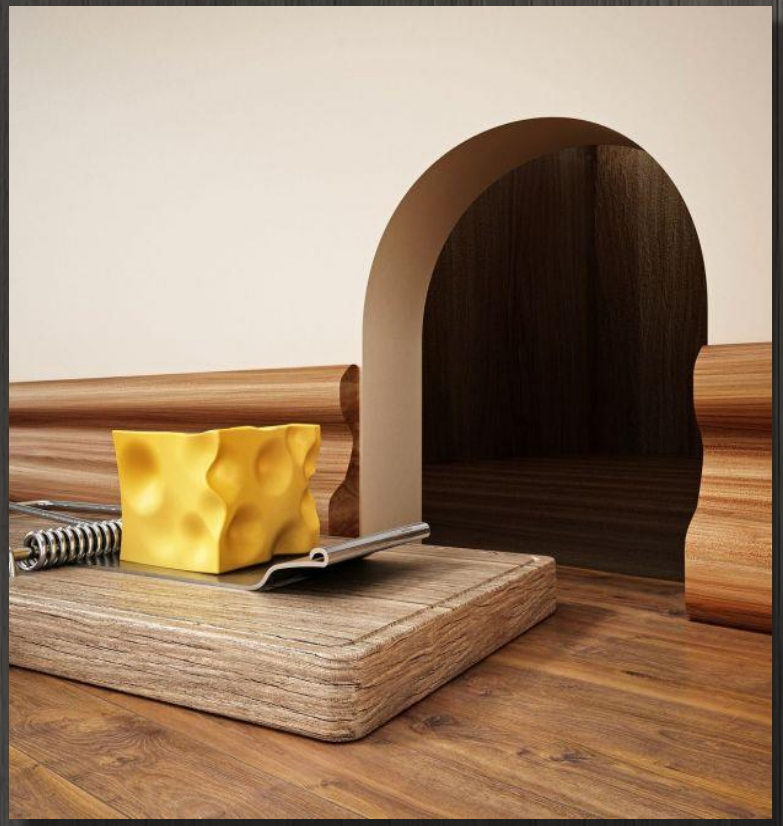
Ej: Simulación de comportamientos

DECEPCION | DESPLIEGUE



REVELAR → PRESENCIA | GUSTOS | CAPACIDADES | VULNERABILIDADES

DEFENSA ACTIVA | BENEFICIOS



1. Detecta todas las amenazas de alto riesgo

APTs, ransomware, AD attacks, análisis predictivo, …

2. Detecta en tiempo real

Mejora de los tiempos de respuesta a incidentes

3. Mínimiza la tasa de falsos positivos

Mejora en la productividad de los defensores (Blueteam)

4. Completa nuestra visibilidad

Cubre cada VLAN, DMZ, endpoint, …

5. Cubre completamente la kill-chain

Menor TCO y mayor sencillez de operaciones

CYBER KILL CHAIN | DECEPTION CHAIN

Collect Intelligence

LIE

1 Reconocimiento

DIVERT

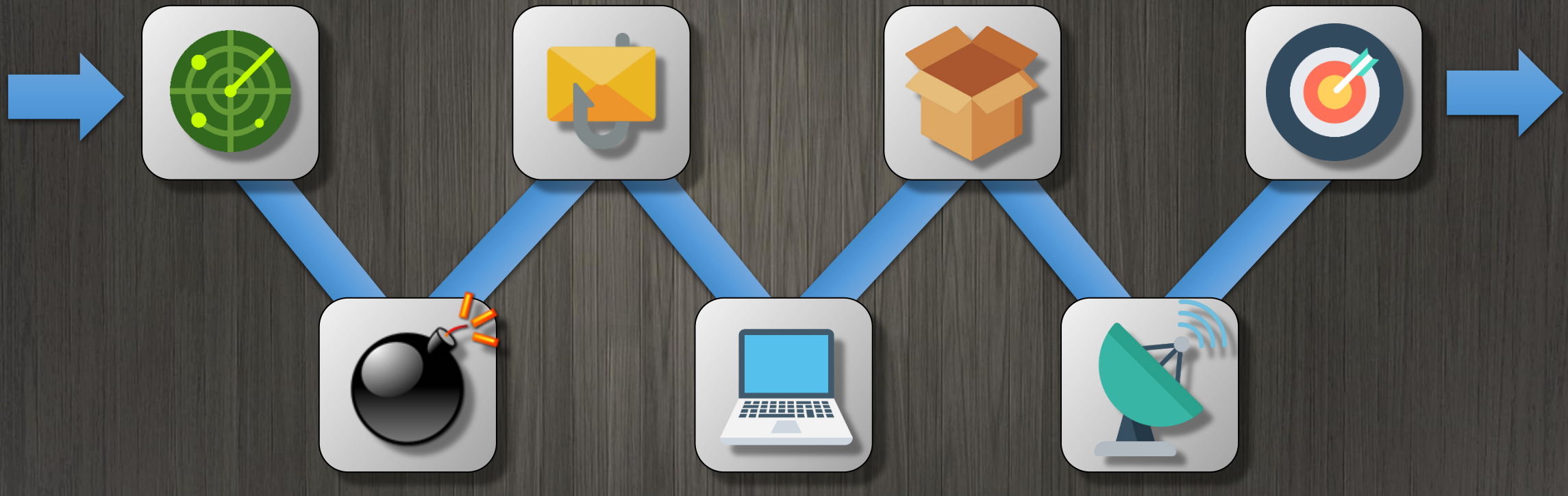
3 Entrega

OBFUSCATE

5 Instalación

DELAY

7 Acciones sobre objetivo



2 Armado

MISDIRECT

Cover Story

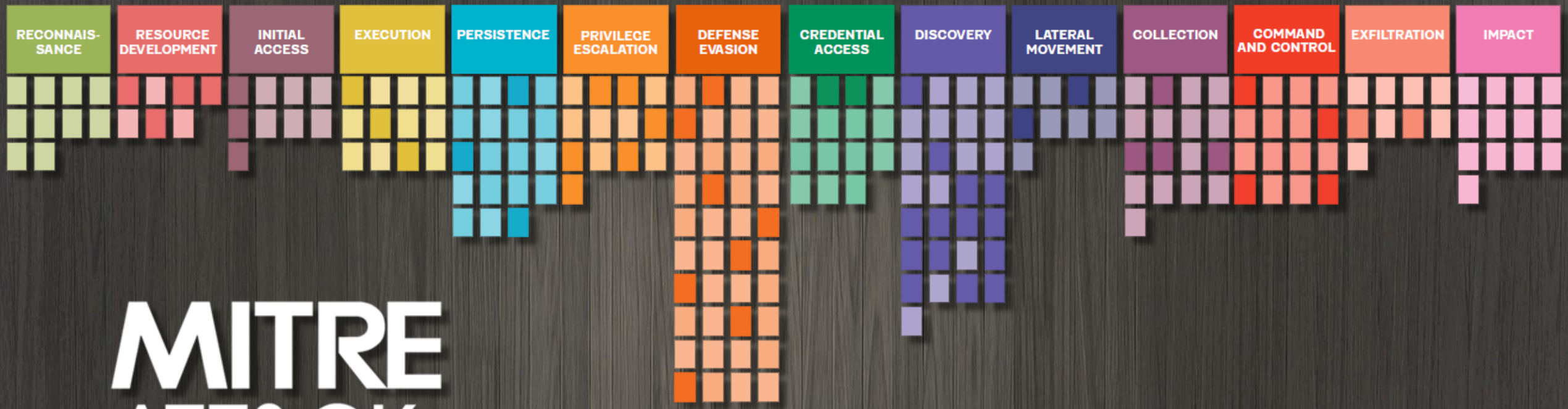
4 Explotación

DECEIVE

6 Comm. & Control

DISRUPT

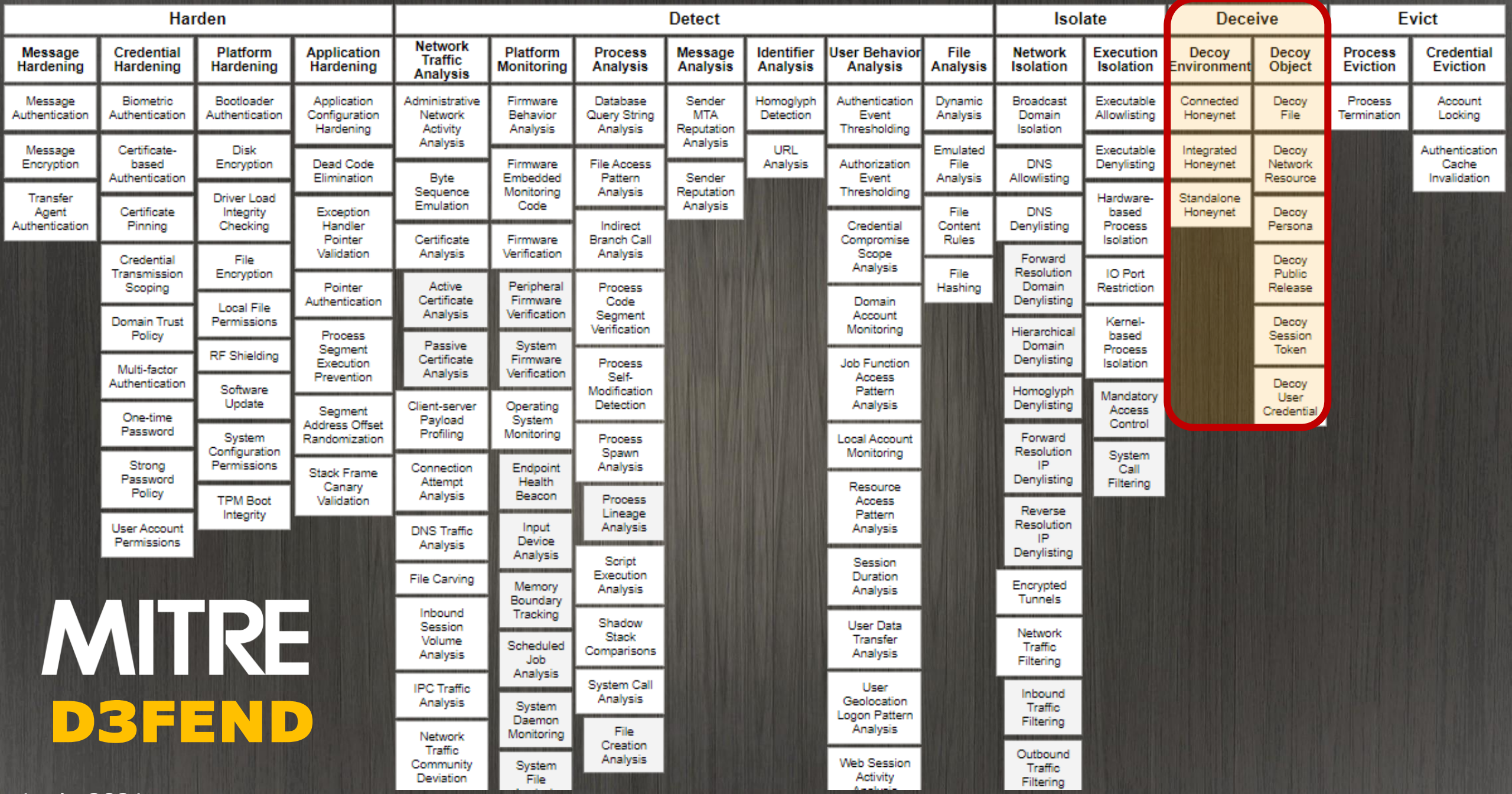
EL METODO | matriz MITRE ATT&CK



MITRE ATT&CK™

FIN8

REvil



MITRE D3FEND

Junio 2021

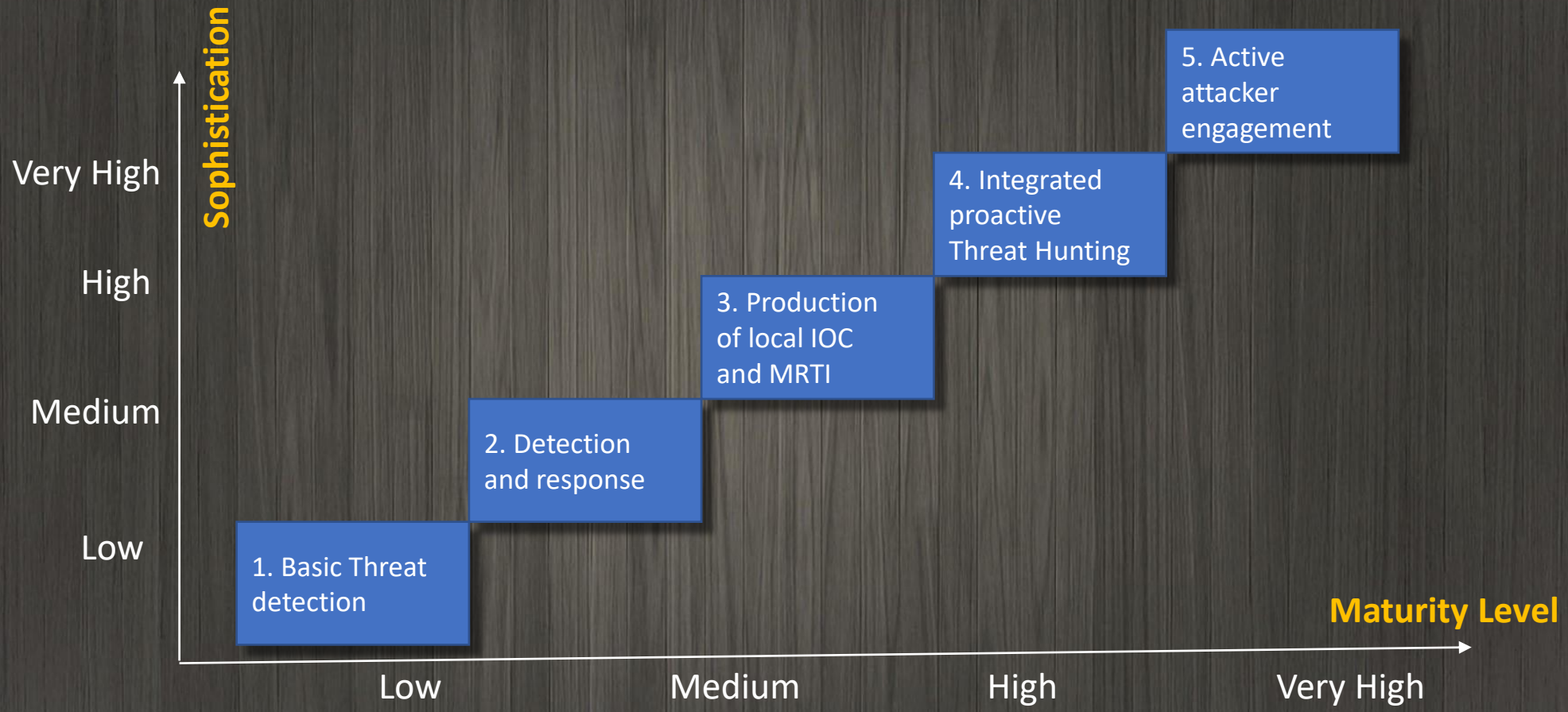
PREPARE	EXPOSE		AFFECT			ELICIT		UNDERSTAND
PLAN	**Collect**	**Detect**	**Prevent**	**Direct**	**Disrupt**	**Reassure**	**Motivate**	**Analyze**
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Decoys	Hardware Manipulation	Email Manipulation	Decoys	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Decoys	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Story boarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

MITRE | Engage™

Febrero 2022

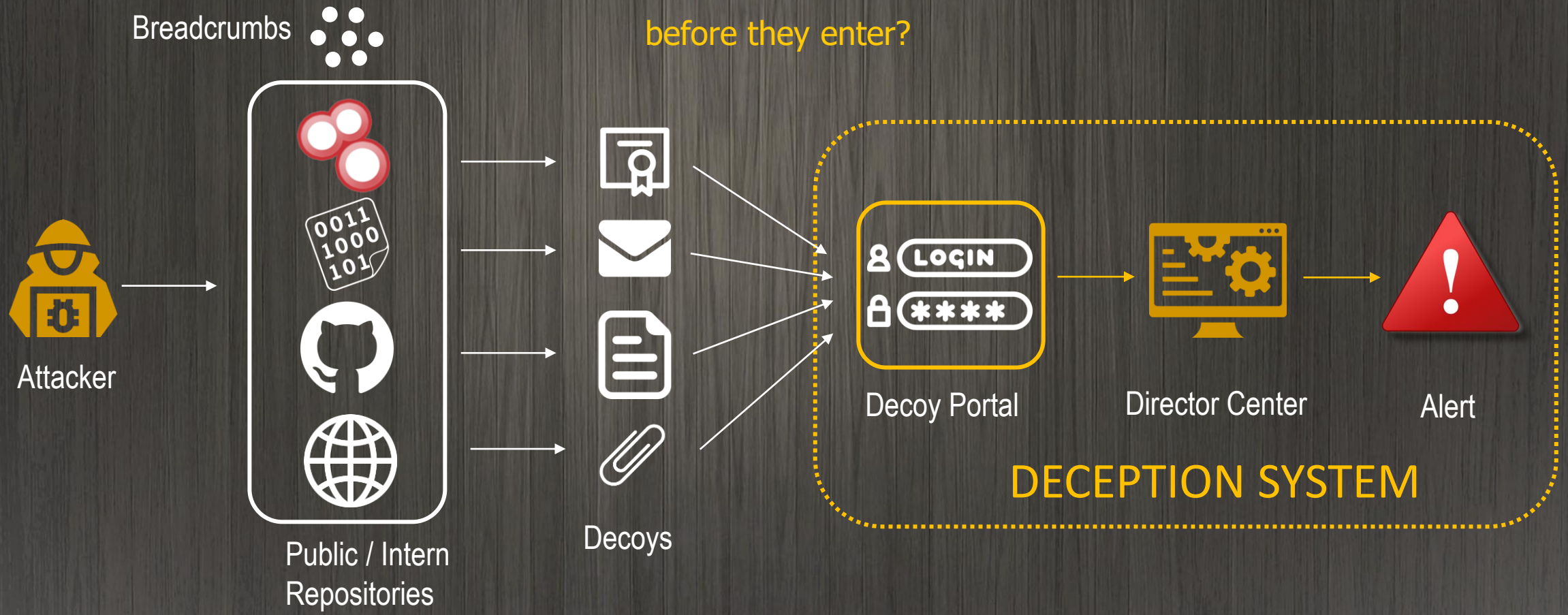
DEMO TIME

NIVELES DE USO: 4+1



CASOS DE USO | Basic detection

```
emilio@miServer:~$ nc -l -k -p 23 > te_pillé.txt
```



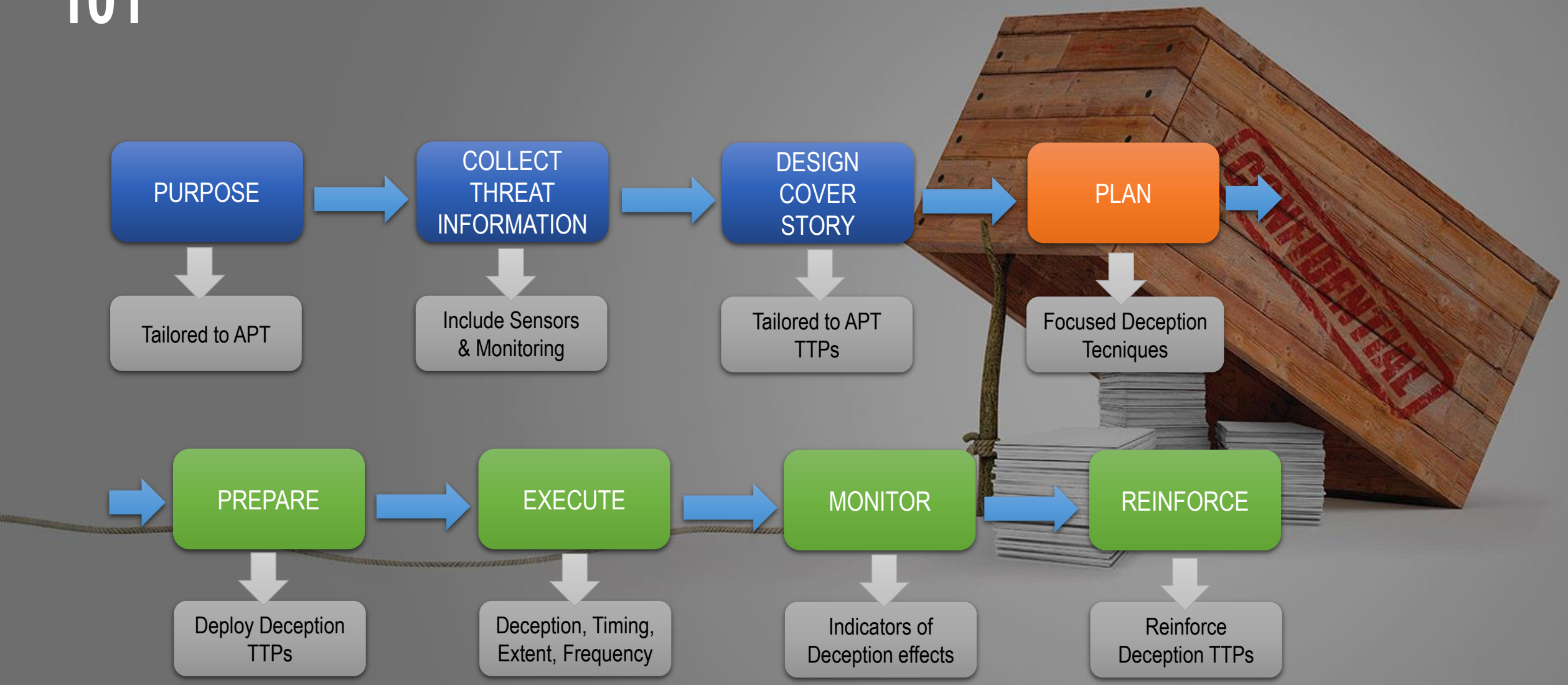
CASOS DE USO | Cloned Web Site Token Script

```
if (document.domain != "https://www.navajanegra.com" &&
document.domain != "https://www.navajanegra.com")
  {
     var l = location.href;
     var r = document.referrer;
     var m = new Image();
     m.src = "https://canarytokens.com/"+
        "ztn3ln88ldw42axqmgnec1cr2.jpg?l="+
         encodeURI(l) + "&amp;amp;r=" + encodeURI(r);
  }
```

https://canarytokens.org

SI QUIERES CAZAR TIBURONES, NECESITAS USAR EL CEBO CORRECTO

ESTRATEGIA DE DECEPCION 101

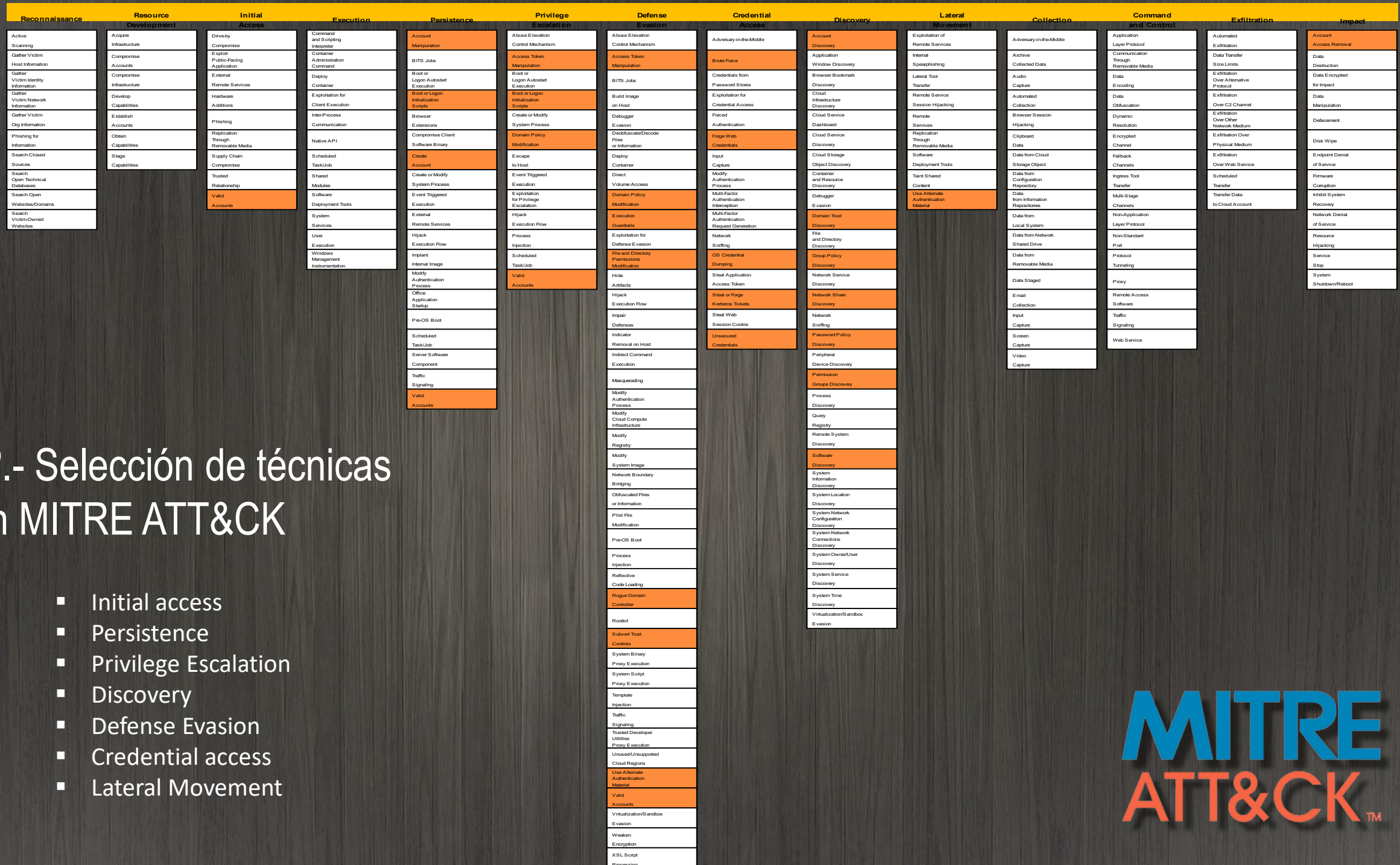


1º

EL PLAN

DA


POR LA COMPRA DE 4 NEUMÁTICOS
SEA CUAL SEA TU
SEXO
LLÉVATE
GRATIS
EL LAVADO TOTAL DEL VEHÍCULO



2º.- Selección de técnicas en MITRE ATT&CK

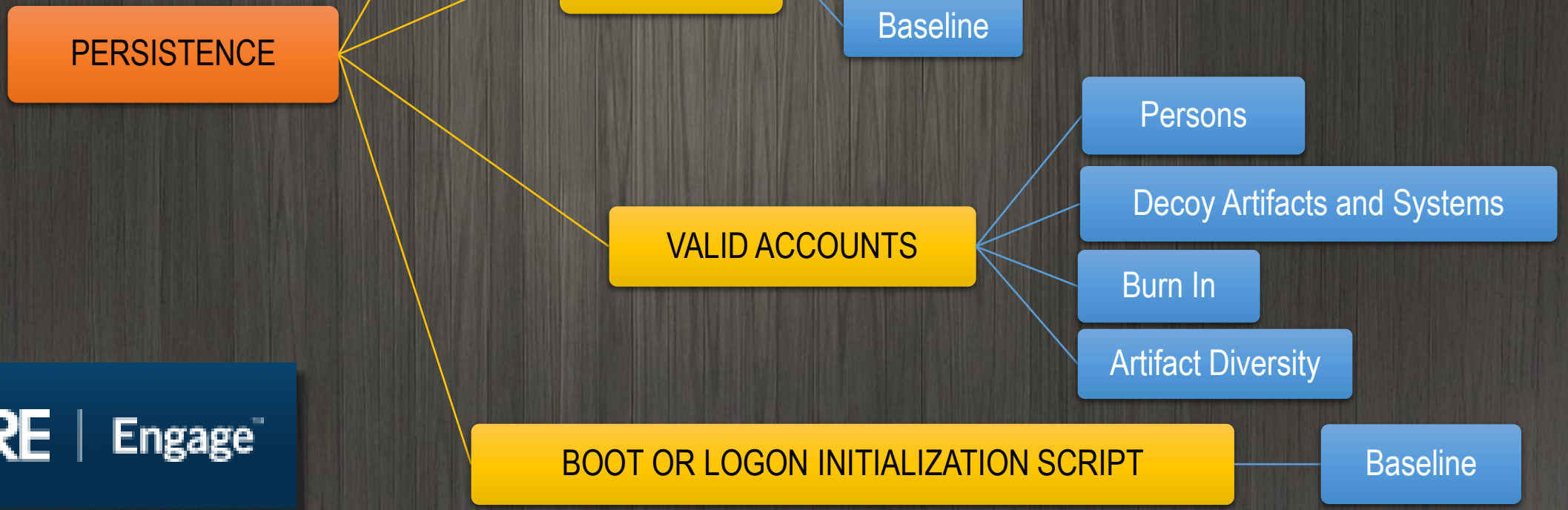
- Initial access
- Persistence
- Privilege Escalation
- Discovery
- Defense Evasion
- Credential access
- Lateral Movement

MITRE ATT&CK™

3º.- Matching Mitre ATT&CK & Engage

- Initial access
- **Persistence**
- Privilege Escalation
- Discovery
- Defense Evasion
- Credential access
- Lateral Movement

MITRE | Engage™



4º.- el escenario | La historia

"No hay nada más engañoso que un hecho obvio" (Sherlock Holmes)

CASOS DE USO | AD Active Defense – 5º. Desplegar la trampa

Active Directory

- Subdomain
- OU
- Users
- GPO

Windows Server

PC1
LSAS UserA

PC2
LSAS UserB

Shared Folders
Web services

New Project X definición.docx

New Project X requisitos.docx

New Project X diseño.docx

.....

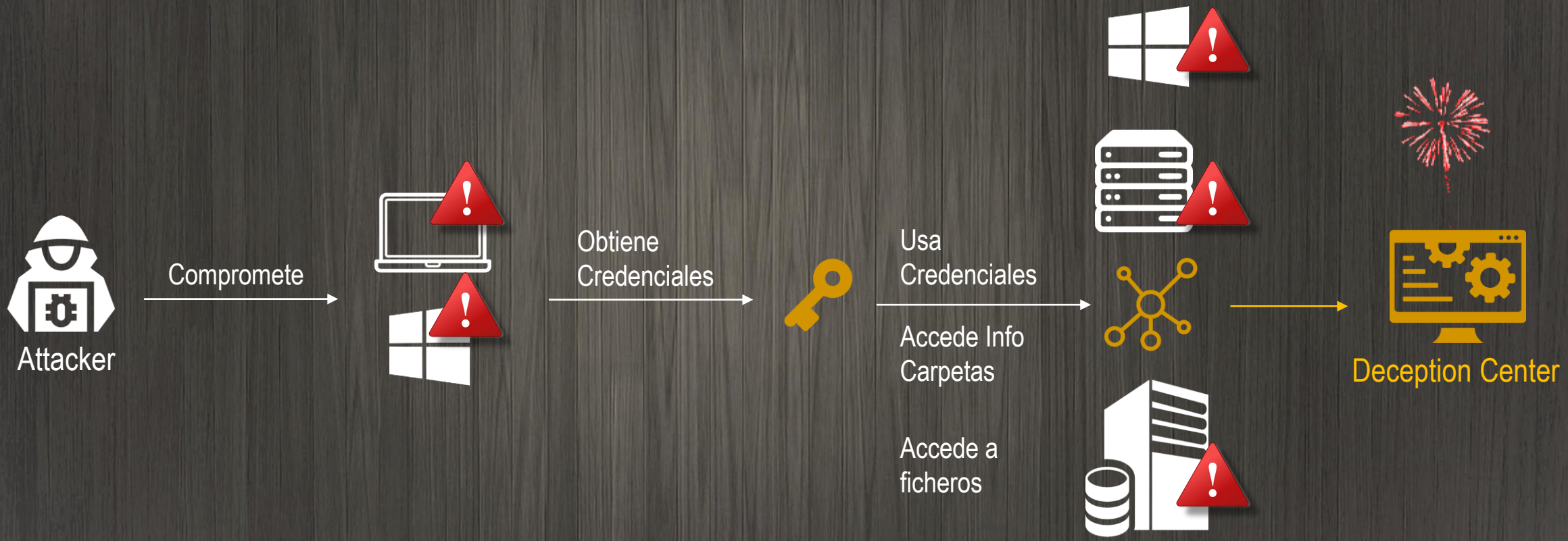
.....

New Project X pruebas.xlsx

Deception
Center

CASOS DE USO | AD Active Defense - 6. Ejecución

Adversary course of action (lo que esperamos que va a ocurrir)



DEMO TIME

red eléctrica

Una empresa de redeia

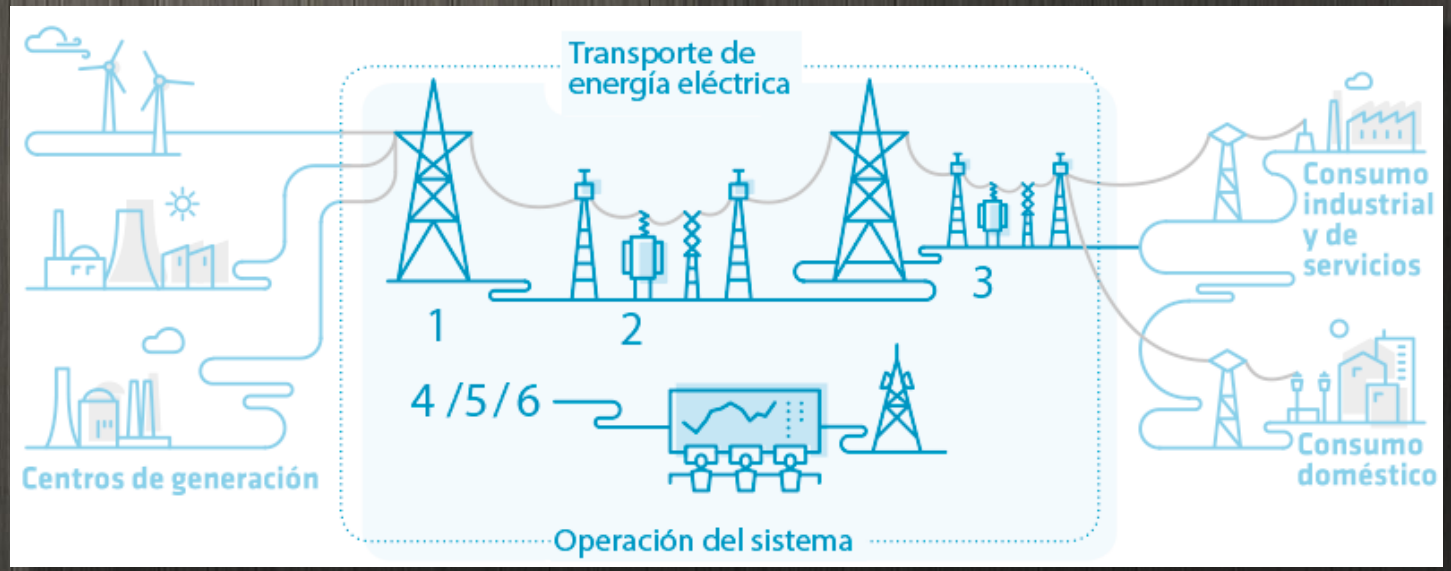
Caso de uso: Honeypot - subestación eléctrica

- Marta Cardenes

red eléctrica

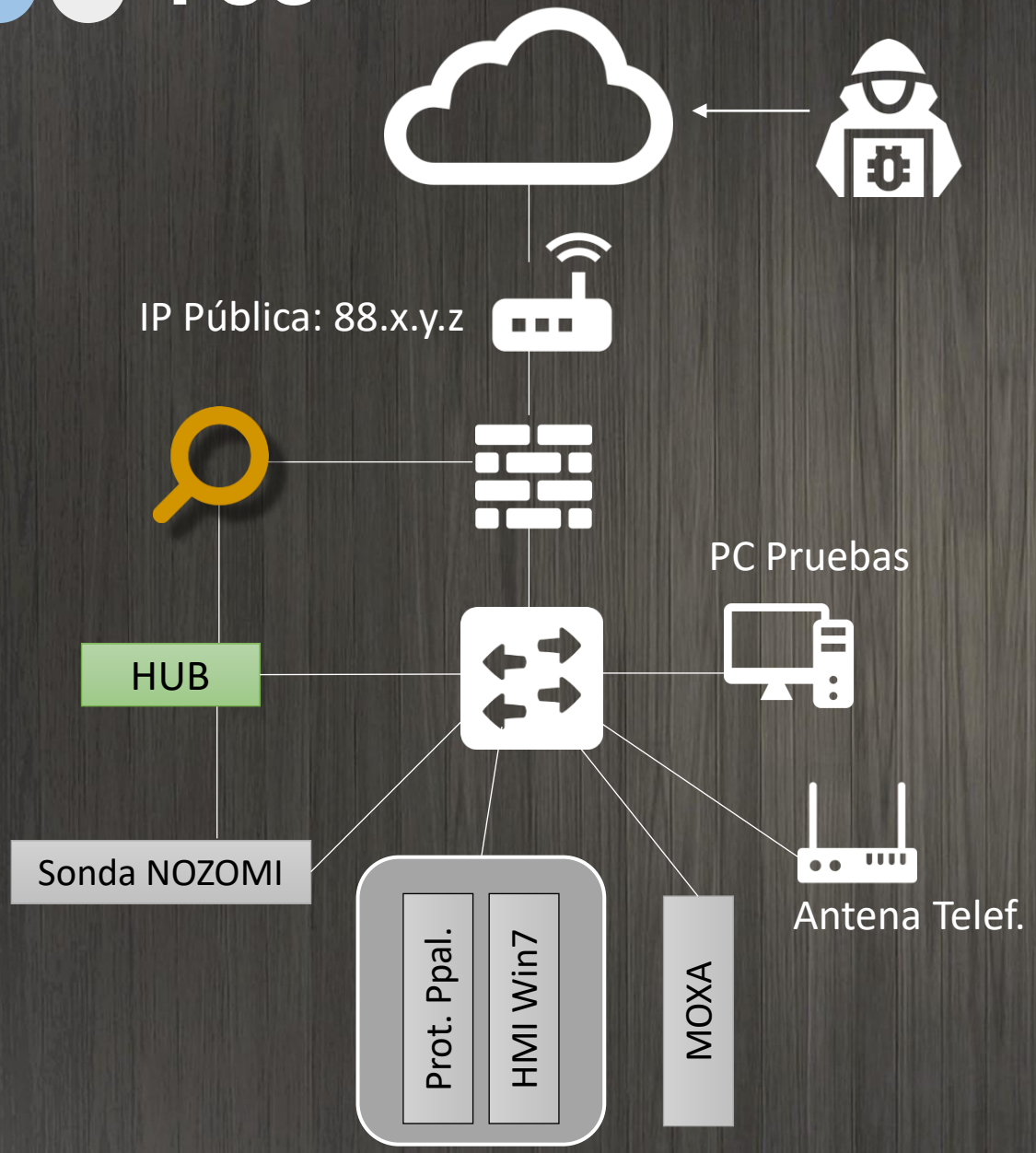
OBJETIVO:

- Descubrir qué ocurriría y como se comportaría un atacante que tuviera la posibilidad de acceder a una subestación eléctrica.



POC

red eléctrica



Poco interés inicial

breadcrumbs

HMI comprometido

red eléctrica

CONCLUSIONES

- Aislamiento en subestaciones
- Bajo interés en otros equipos industriales
- Parametrización IDS óptima
- Evolución a honeypot para el insider

Resumiendo → nuestro objetivo | **engañar**

"Nunca interrumpas a tu enemigo cuando está cometiendo un error"

Napoléon Bonaparte

CONCLUSIONES

- Defensa Activa …
  - Centrada en intenciones, no en herramientas
  - + Proactivo - Reactivo
  - + Detección + Visibilidad - ‘No’ falsos positivos

Componente Clave en los “next-gen SOC”

NO SUBVALORAR LA AMENAZA !!

MUCHAS GRACIAS

Emilio Rico Ruiz

GRUPO TRC®

TOMAS FALSAS

MASTERING CIBER DECEPTION

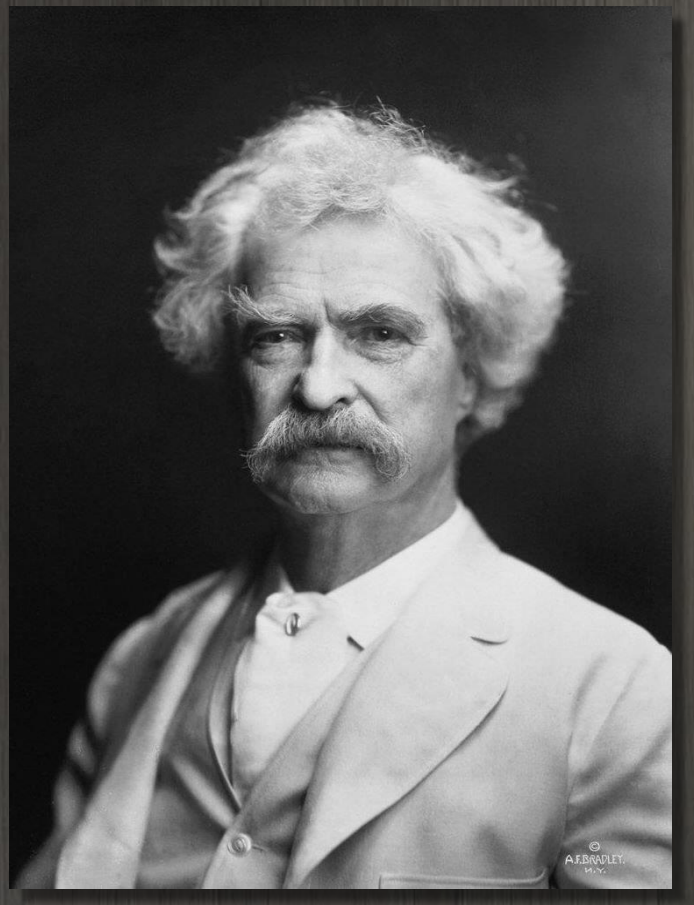
TOMAS FALSAS

DECEPTION

- ¿A quien va usted a creer, a mí o a sus propios ojos?

TOMAS FALSAS

DECEPTION - Mark Twain



- Es más fácil engañar a la gente que convencerlos de que han sido engañados
- Nunca le digas la verdad a la gente que no es digna de ella

TOMAS FALSAS

DECEPTION

“Los criminales no son complicados. Solo tienes que averiguar lo que están buscando.”

Batman - the Dark Knight (2008)

TOMAS FALSAS

CIBER-SUN-TZU

The Art of War, c. 500 BC

- El arte de la ciber-guerra se basa en el engaño
- Haz que los hackers vean mis fortalezas como debilidades y mis debilidades como NextGen-Firewalls, mientras hago que sus fortalezas se conviertan en debilidades y descubro sus TTP,s
- Debemos fingir ser exploitables, para que el enemigo se pierda en la arrogancia
- Un Blue-Team victorioso gana primero y entabla la batalla después

Cliffor Stoll, autor de ‘El huevo del cuco’

TOMAS FALSAS

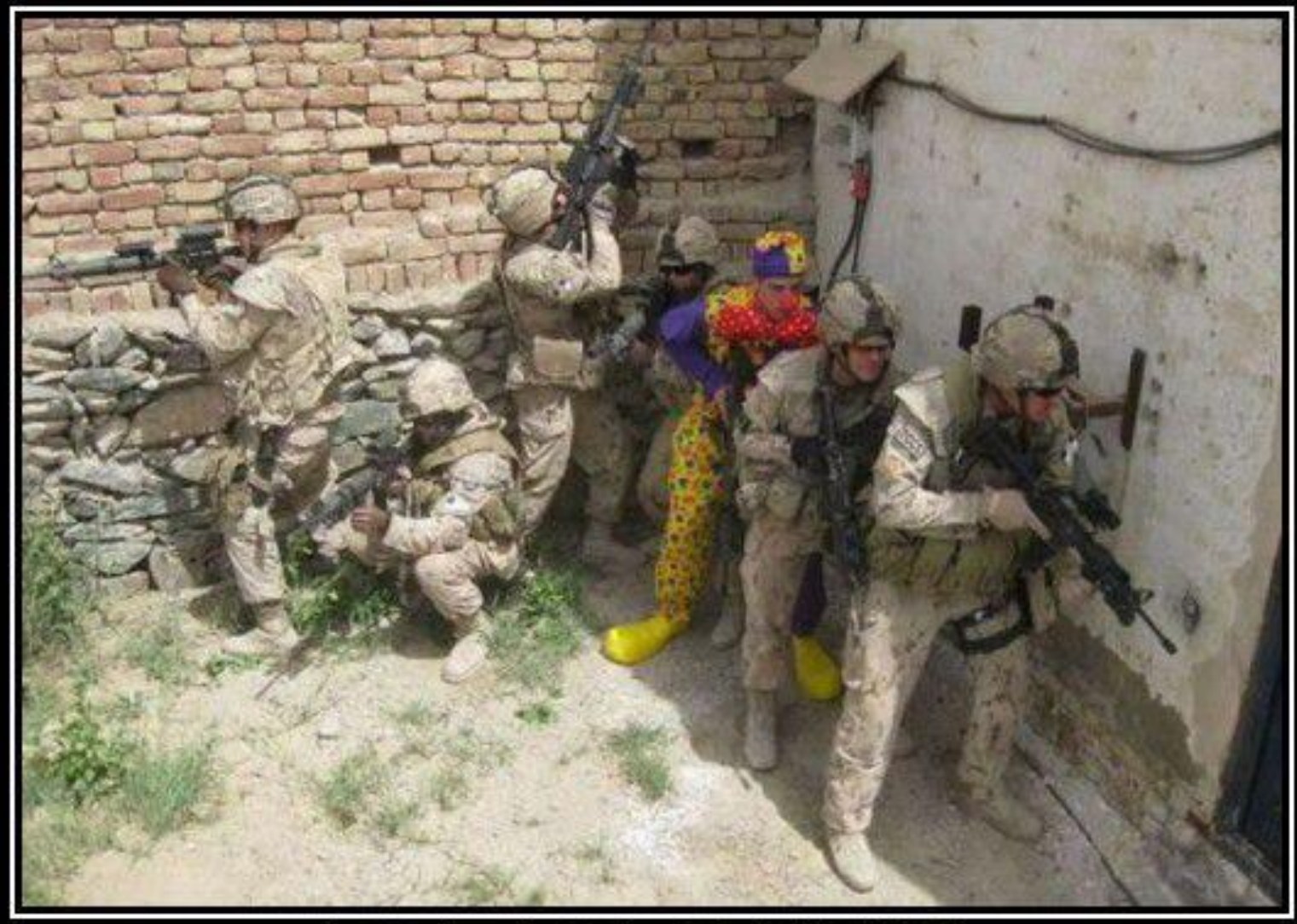
DECEPTION

En una galaxia muy lejana

- ‘Estos nos son los **SERVERS** que estáis buscando’

TOMAS FALSAS

Make a believable story



DECOY'S

In military use since 300 BC.

BIBLIOGRAFIA

LIBROS

Deception in War - Jon Latimer
El Huevo Del Cuco - Clifford Stoll
The Art of Deception - Kevin Mitnick

ESTUDIOS E INFORMES

Cyber Denial, Deception and Counter Deception - Kristin Heckman, Frank Stech
A guide to designing deceptive action - NCDL
Three Decades of Deception Techniques in Active Cyber Defense - Li Zhang
Deception Techniques Using Honeypots - Amit Lakhani
A theory of Deceptive Cybersecurity - Richard Baskerville, Pengcheng Wang
Cyber Deception Approach and education for Resilience in Hybrid Threats Model - Steingartner
Towards Cyber Attribution by Deception - Sampsa Ranti
Design Thinking for Cyber Deception - Debi Ashenden, Robert Black

GUÍAS

Guia de implantación de un honeypot industrial - INCIBE
Implementer's guide to Deception Technologies - Kyle Dickinson (SANS)

MUCHAS GRACIAS

Emilio Rico Ruiz
Security Advisor