

Y qué más da, si ...

... son cosas de la E.D.A.D



Emilio Rico Ruiz
Grupo TRC

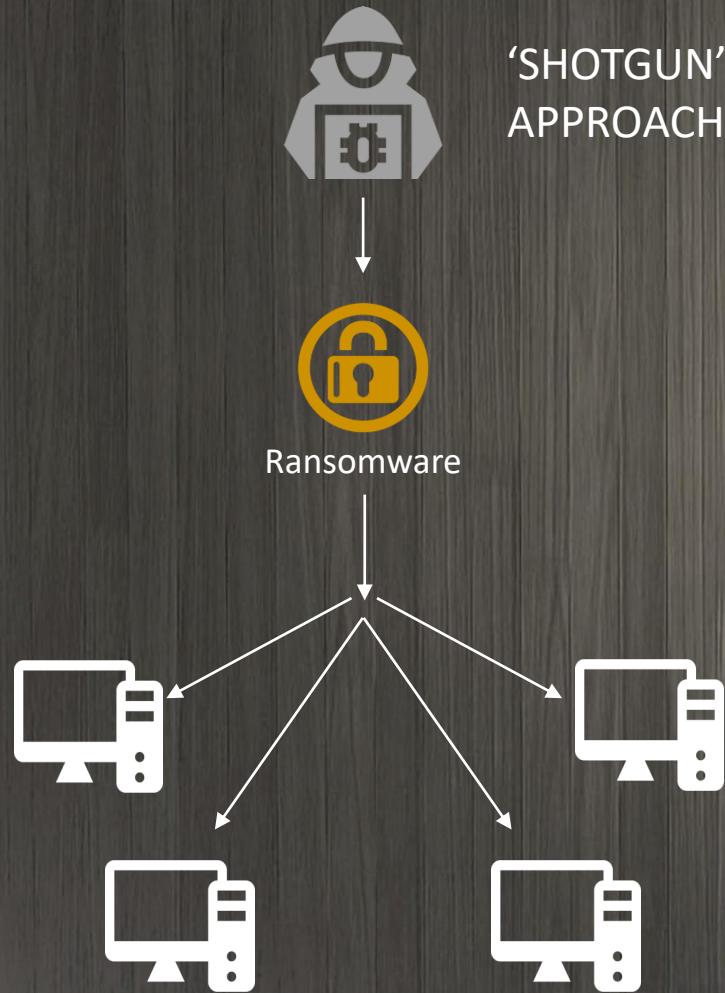
Estrategias de DEFENSA ACTIVA y DECEPCION



Emilio Rico Ruiz
Grupo TRC

DWell Time

(LOS TIEMPOS CAMBIAN)



'SHOTGUN'
APPROACH



POST-COMPROMISO
APPROACH



1st Stage

Credential Theft
Internal reconnaissance
Lateral movement
Escalate privileges
Delete backups



2nd Stage
Ransomware



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.

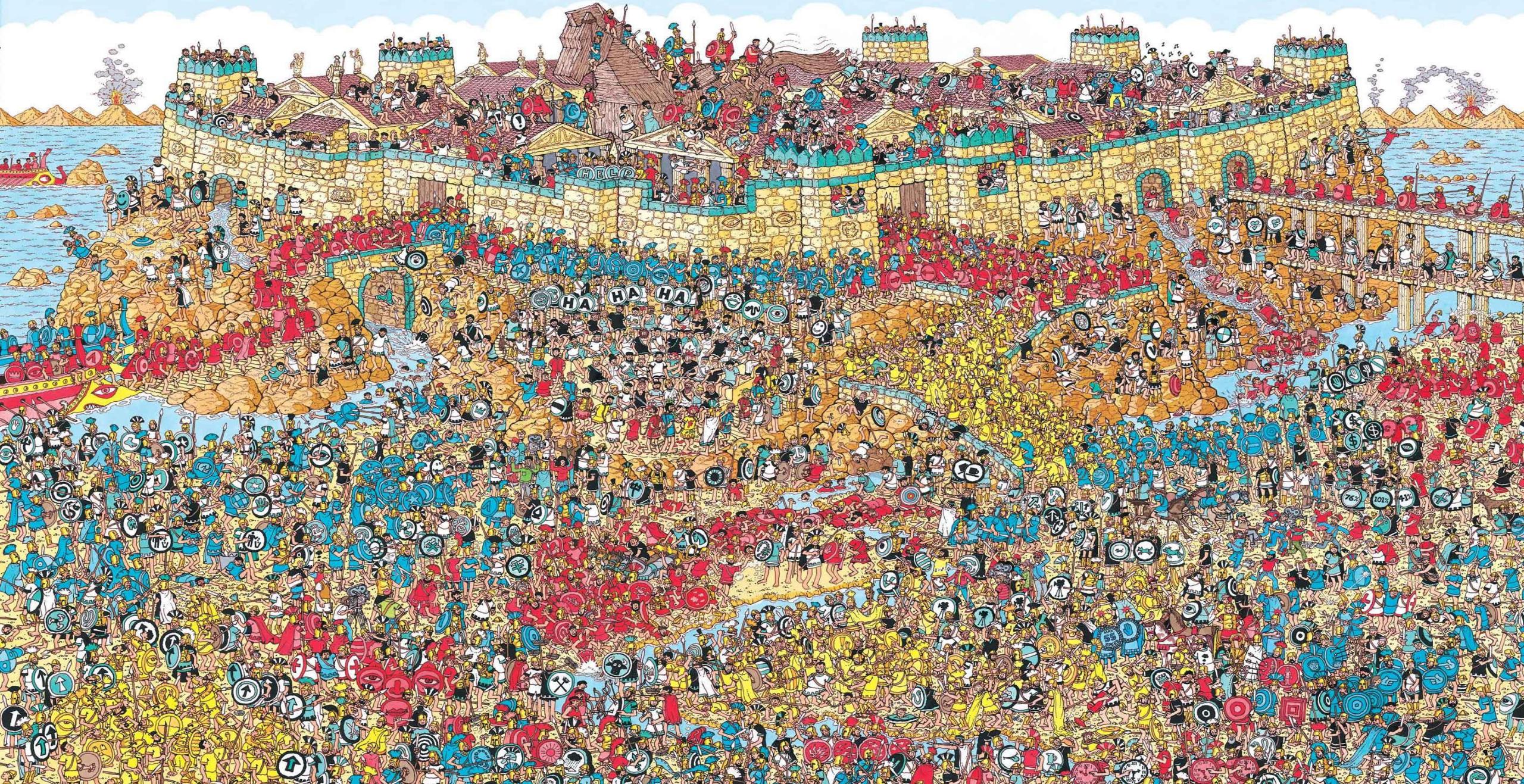
Data breach costs rose from \$3.86 million to \$4.24 million.

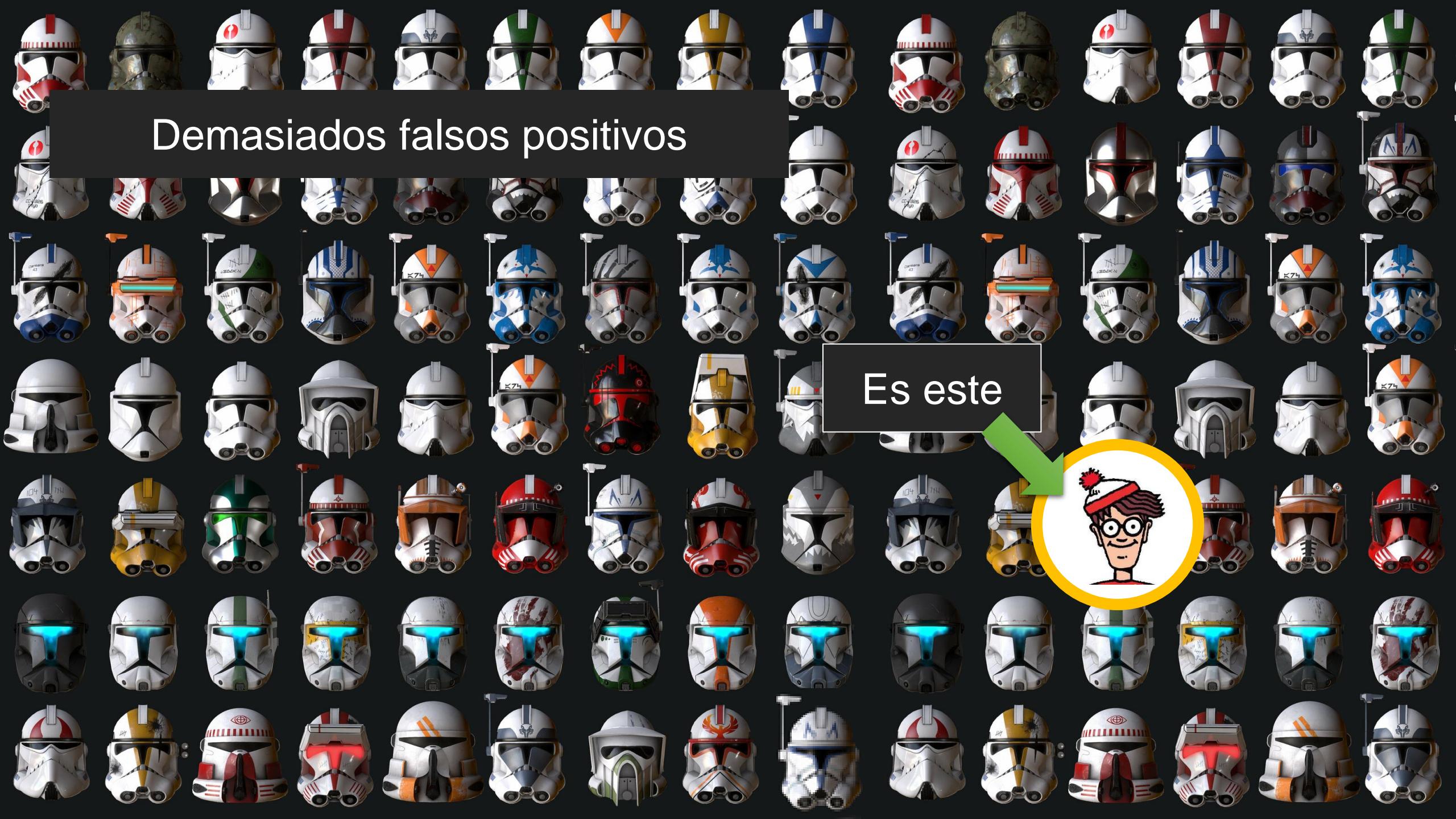
The longer it took to identify and contain, the more costly the breach.

Entorno (siempre) Cambiante



MALA VISIBILIDAD





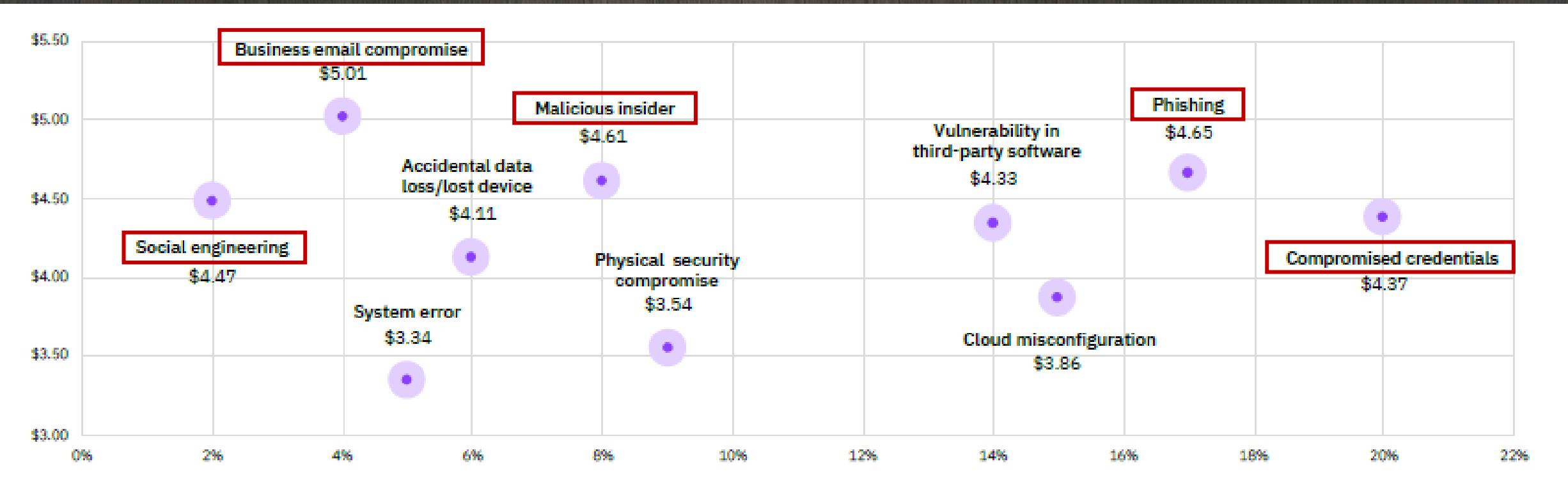
Demasiados falsos positivos

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 ...

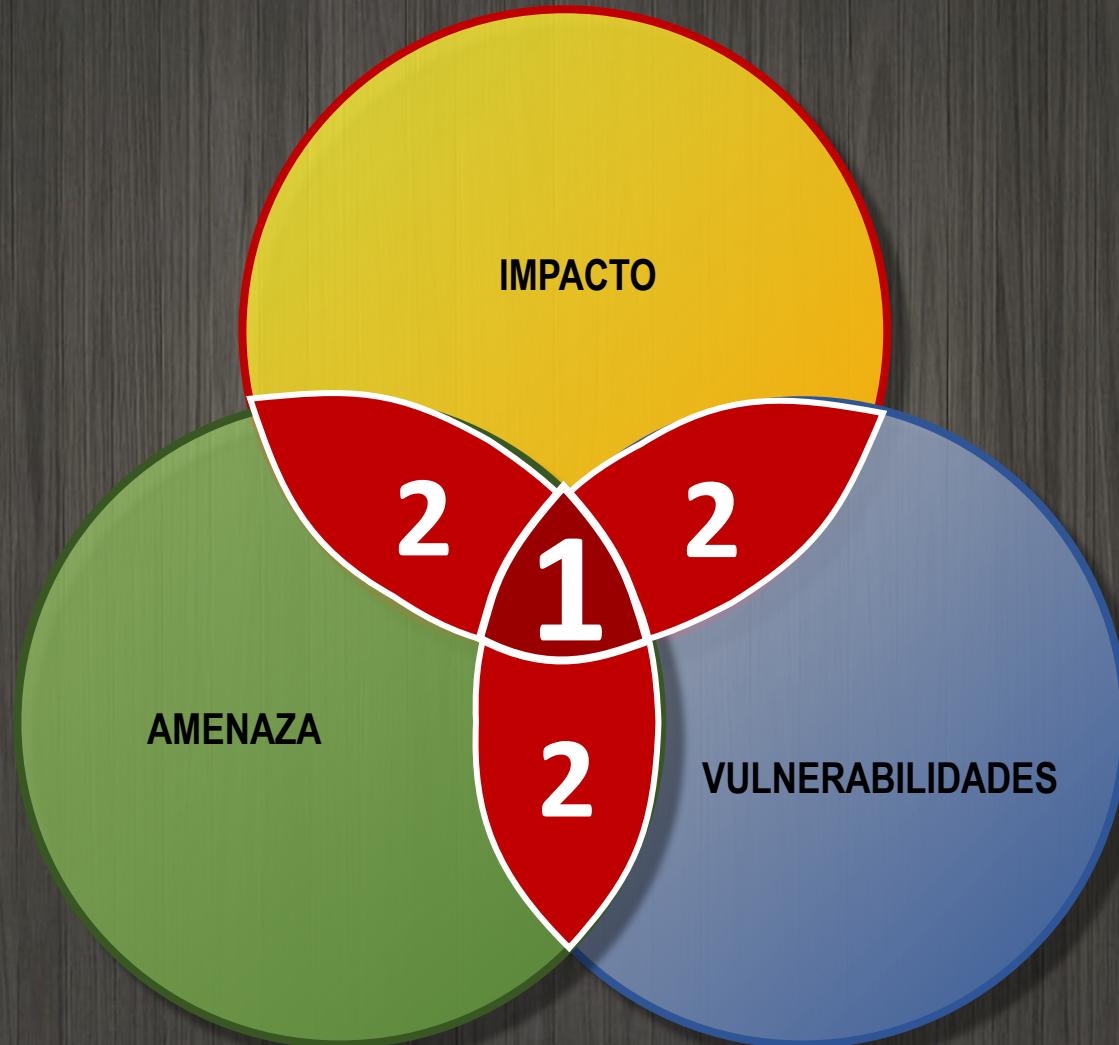
¿Por qué no **cambiamos las reglas del juego?**



100%
↔
1 vez



RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



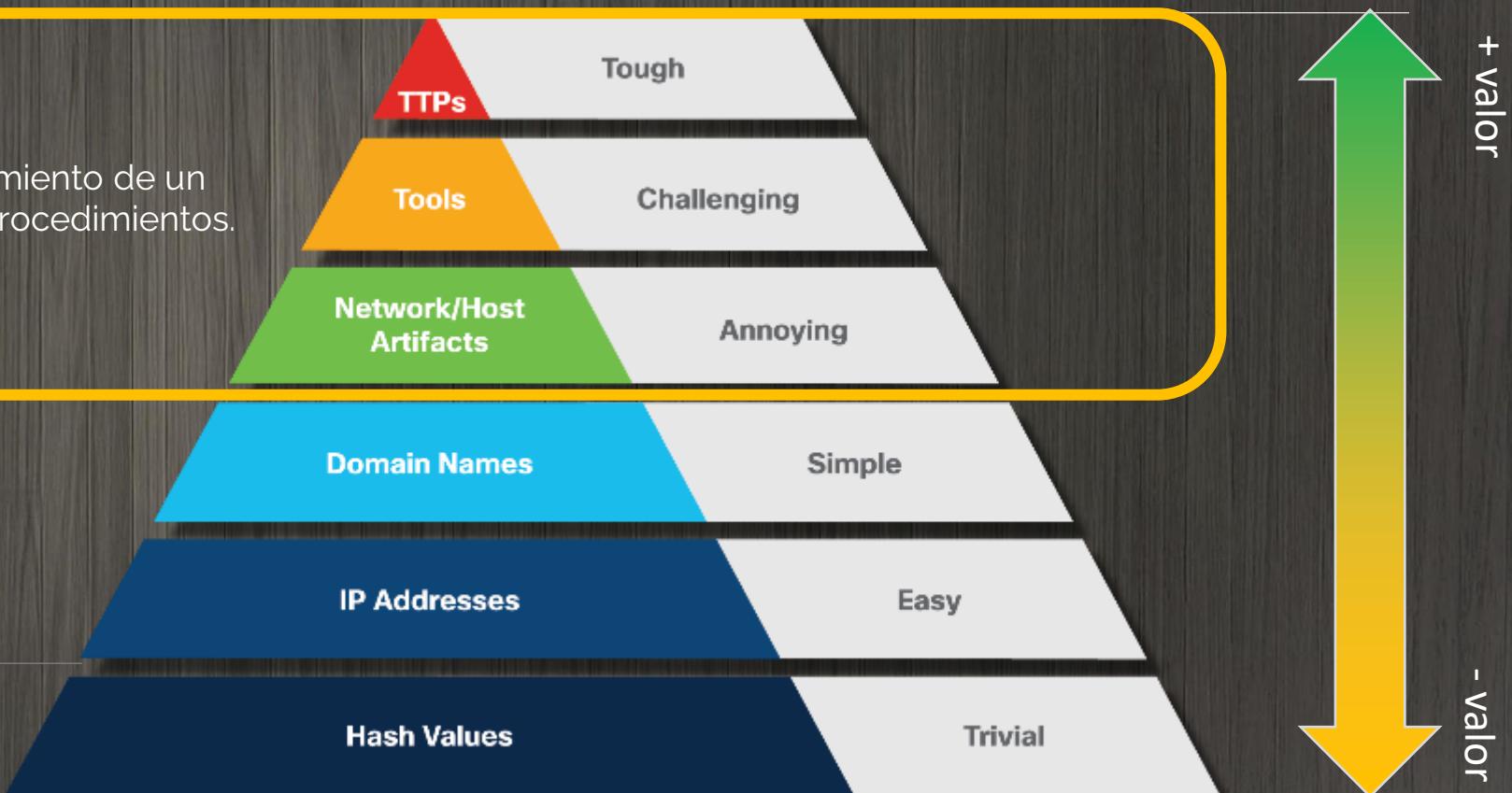
IOC,s

Indicadores conductuales

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

Indicadores atómicos

Indicadores calculados



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

nota :

SEÑOR PADRE

Soy el Maestro

De So Hijo

y no AVRAN

CLASES DURANTE

2 SEMANAS

1

Maestro

[Signature]

Director

+
Diosit



Engaños IV: II WW



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. Zhukov

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



- 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 ciberneticas defensivas





- DEFENSA ACTIVA
- DECEPTION TECHNOLOGIES



DECEPCION | Cómo funciona?



CAMPAÑA
ESTRATEGIA



HOST &
SERVICES

trampas, sueños ...



BREADCRUMBS

MIGAS DE PAN

¿INCENTIVOS?



DEFENSA ACTIVA vs HONEY | No es lo mismo**

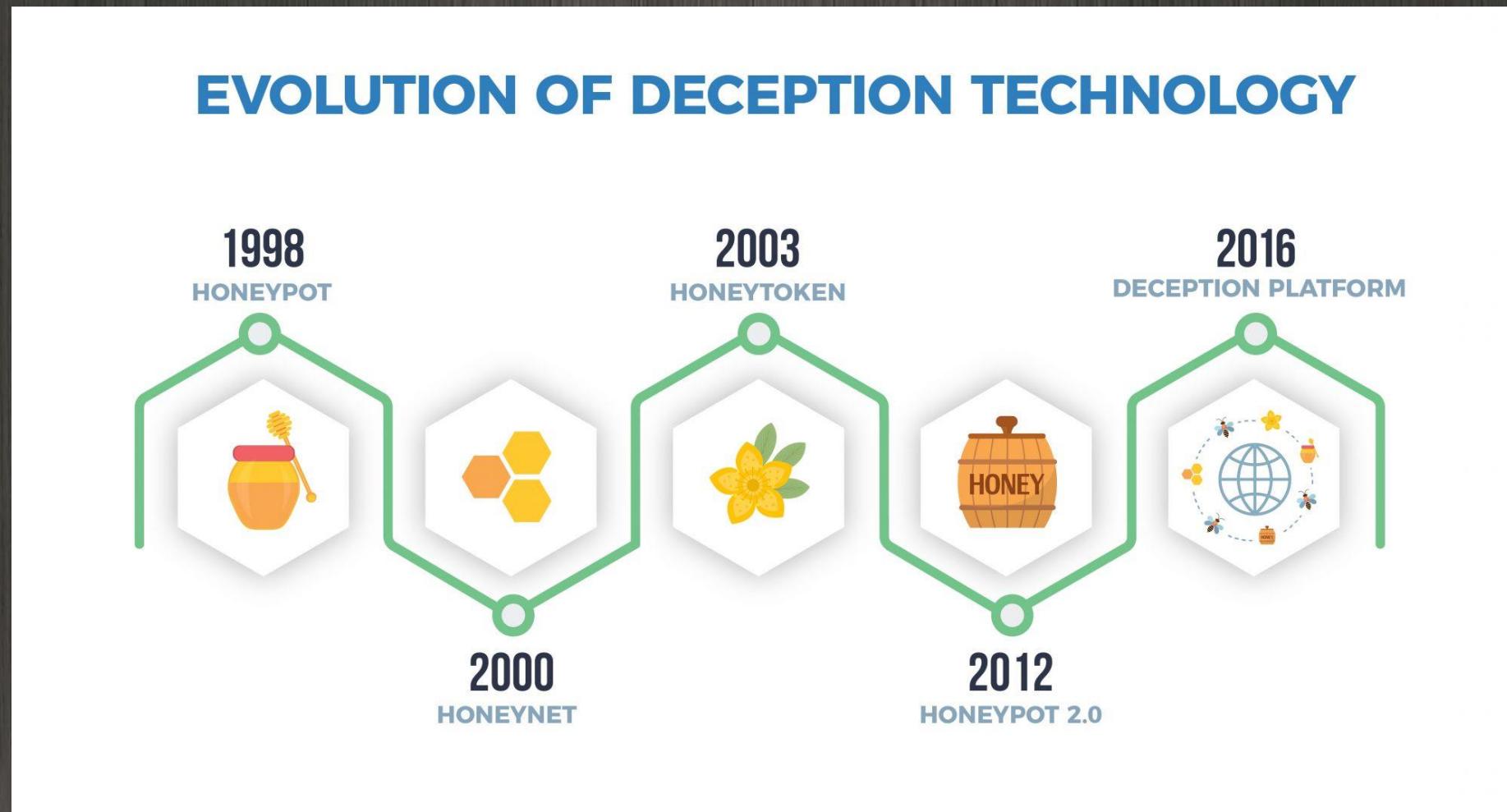
Honeypots / Honeynets ...

- 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

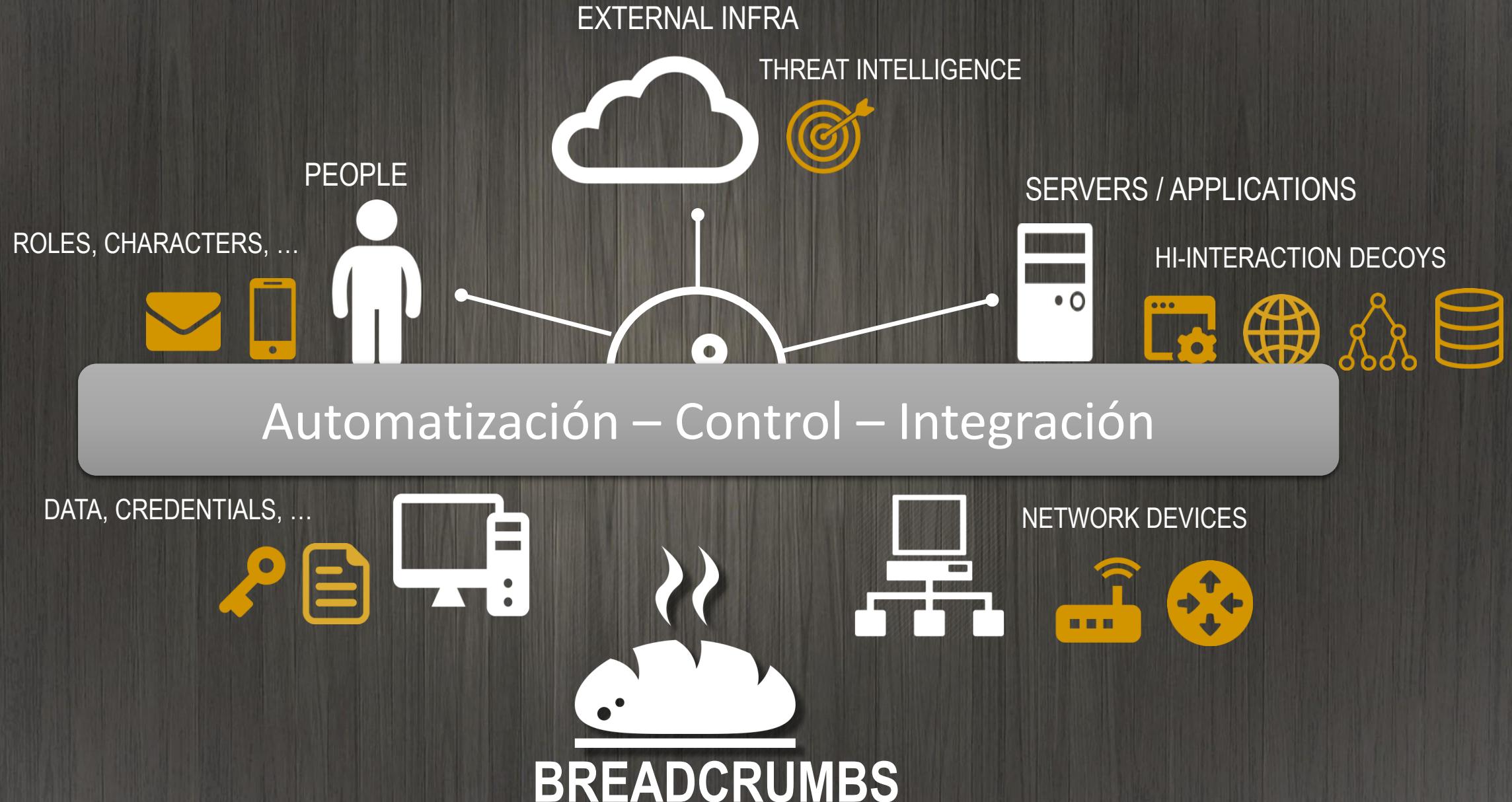


RQ,s

- 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.

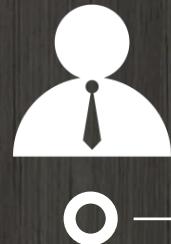


DECEPCION | COMPONENTES

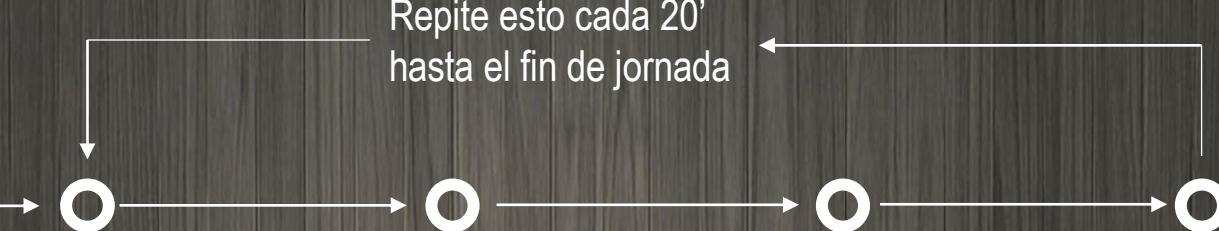


DEFENSA ACTIVA | Soportado por IA

Ej: Simulación de comportamientos



Haz loggin en la red con el usuario deseado



Repite esto cada 20' hasta el fin de jornada



Repite cada día hasta el final de la campaña

Navega un poco para crear una historia

Ejecuta unos pocos comandos

Accede a una BD de la empresa

Teclea y/o ejecuta cualquier otra actividad normal



Añadir servicio



Seleccionar comportamiento

Añadir credenciales

Activar servicio



INFLUENCIA

DECEPCION | DESPLIEGUE



REVELAR → PRESENCIA | GUSTOS | CAPACIDADES | VULNERABILIDADES

DEFENSA ACTIVA | BENEFICIOS

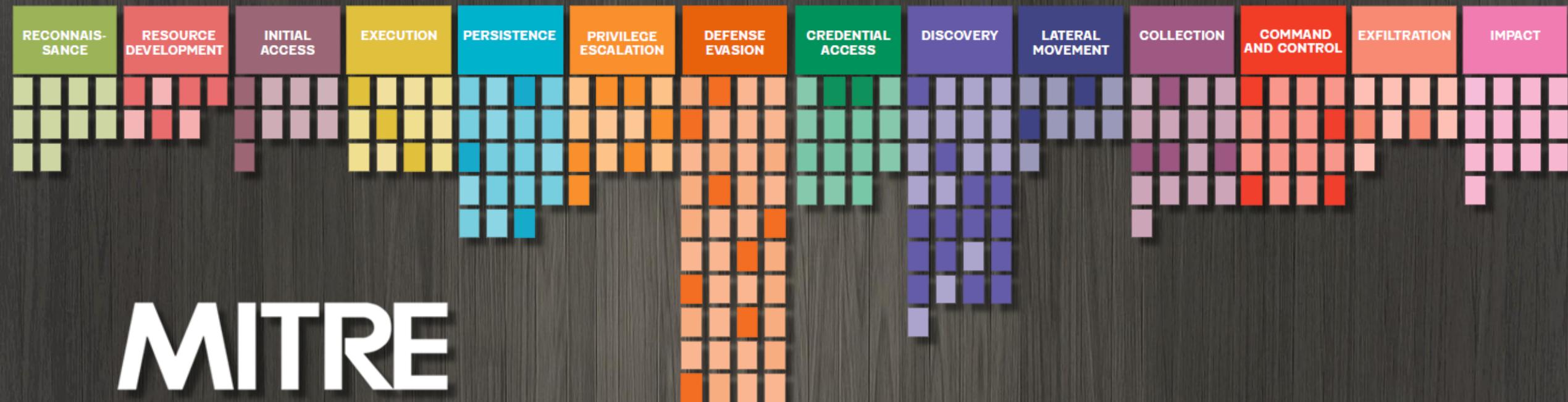


- 1. Detecta todas las amenazas de alto riesgo**
APTs, ransomware, AD attacks, análisis predictivo, ...
- 2. Detecta en tiempo real**
Mejora de los tiempos de respuesta a incidentes
- 3. Mínimiza la tasa de falsos positivos**
Mejora en la productividad de los defensores (Blueteam)
- 4. Completa nuestra visibilidad**
Cubre cada VLAN, DMZ, endpoint, ...
- 5. Cubre completamente la kill-chain**
Menor TCO y mayor sencillez de operaciones

CYBER KILL CHAIN | DECEPTION CHAIN



EL METODO | matriz MITRE ATT&CK



MITRE ATT&CK™



REvil



Harden				Detect								Isolate		Deceive		Evict	
Message Hardening	Credential Hardening	Platform Hardening	Application Hardening	Network Traffic Analysis	Platform Monitoring	Process Analysis	Message Analysis	Identifier Analysis	User Behavior Analysis	File Analysis	Network Isolation	Execution Isolation	Decoy Environment	Decoy Object	Process Eviction	Credential Eviction	
Message Authentication	Biometric Authentication	Bootloader Authentication	Application Configuration Hardening	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Sender MTA Reputation Analysis	Homoglyph Detection	Authentication Event Thresholding	Dynamic Analysis	Broadcast Domain Isolation	Executable Allowlisting	Connected Honeynet	Decoy File	Process Termination	Account Locking	
Message Encryption	Certificate-based Authentication	Disk Encryption	Dead Code Elimination	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Sender Reputation Analysis	URL Analysis	Authorization Event Thresholding	Emulated File Analysis	DNS Allowlisting	Executable Denylisting	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation		
Transfer Agent Authentication	Certificate Pinning	Driver Load Integrity Checking	Exception Handler Pointer Validation	Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Sender Reputation Analysis	URL Analysis	Credential Compromise Scope Analysis	File Content Rules	DNS Denylisting	Hardware-based Process Isolation	Standalone Honeynet	Decoy Persona			
Credential Transmission Scoping		File Encryption	Pointer Authentication	Active Certificate Analysis	Peripheral Firmware Verification	Process Code Segment Verification			Domain Account Monitoring	File Hashing	Forward Resolution Domain Denylisting	IO Port Restriction		Decoy Public Release			
Domain Trust Policy		Local File Permissions	Process Segment Execution Prevention	Passive Certificate Analysis	System Firmware Verification	Process Self-Modification Detection			Job Function Access Pattern Analysis		Hierarchical Domain Denylisting	Kernel-based Process Isolation		Decoy Session Token			
Multi-factor Authentication		RF Shielding	Software Update	Segment Address Offset Randomization	Client-server Payload Profiling	Operating System Monitoring			Local Account Monitoring		Homoglyph Denylisting	Mandatory Access Control		Decoy User Credential			
One-time Password			System Configuration Permissions	Stack Frame Canary Validation	Connection Attempt Analysis	Endpoint Health Beacon			Resource Access Pattern Analysis		Forward Resolution IP Denylisting	System Call Filtering					
Strong Password Policy				DNS Traffic Analysis	Input Device Analysis	Process Lineage Analysis			Session Duration Analysis		Reverse Resolution IP Denylisting						
User Account Permissions				File Carving	Memory Boundary Tracking	Script Execution Analysis			User Data Transfer Analysis		Encrypted Tunnels						
				Inbound Session Volume Analysis	Scheduled Job Analysis	Shadow Stack Comparisons					Network Traffic Filtering						
				IPC Traffic Analysis	System Call Analysis	System Daemon Monitoring			User Geolocation Logon Pattern Analysis		Inbound Traffic Filtering						
				Network Traffic Community Deviation	System File	File Creation Analysis			Web Session Activity Analysis		Outbound Traffic Filtering						

MITRE
D3FEND

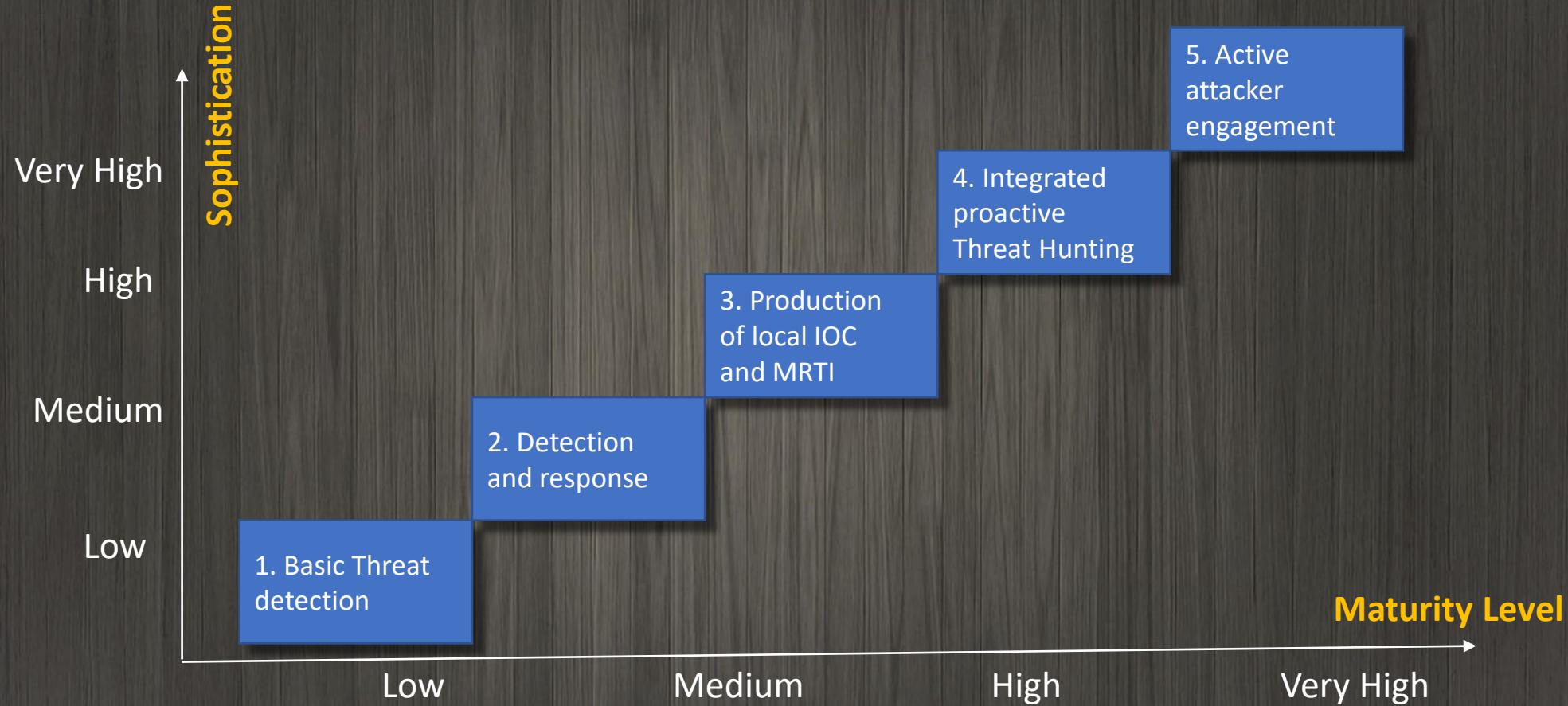
PREPARE	EXPOSE		AFFECT			ELICIT		UNDERSTAND
PLAN	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	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™

DEMO TIME

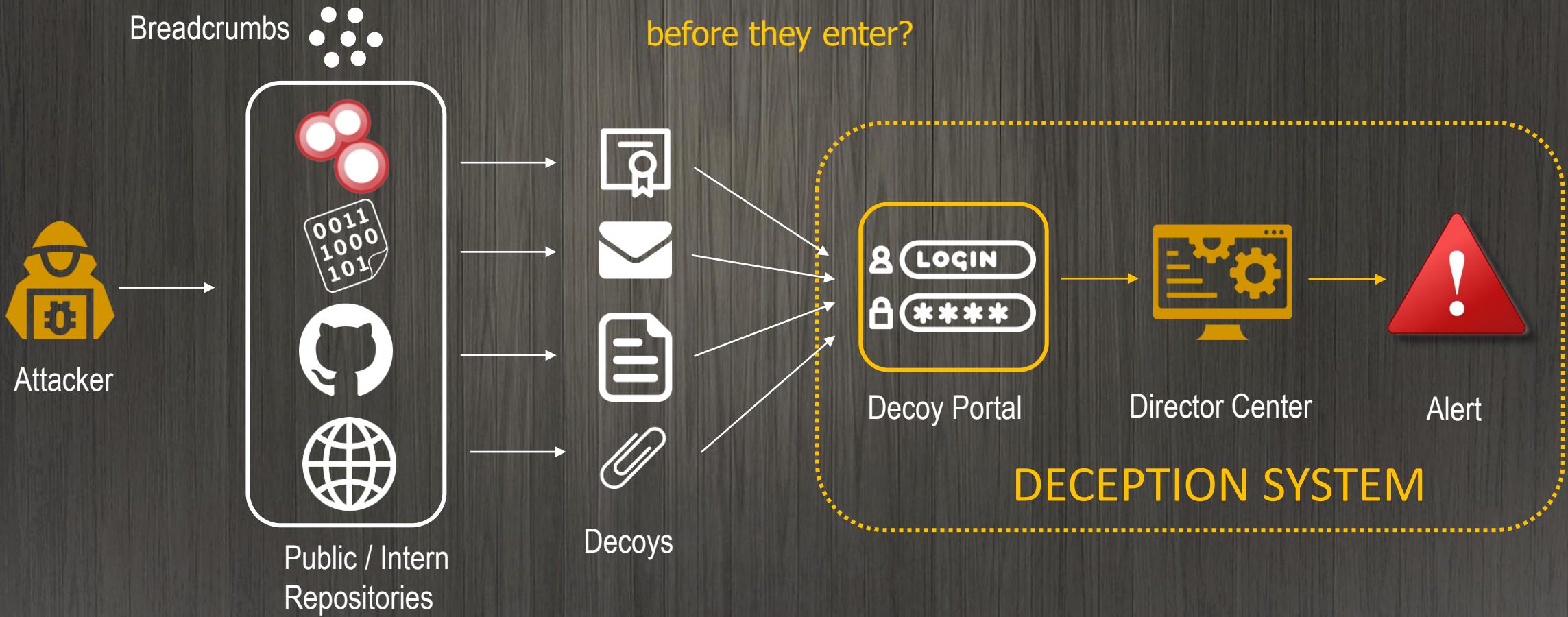


NIVELES DE USO: 4+1



CASOS DE USO | Basic detection

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



CASOS DE USO | Cloned Web Site Token Script



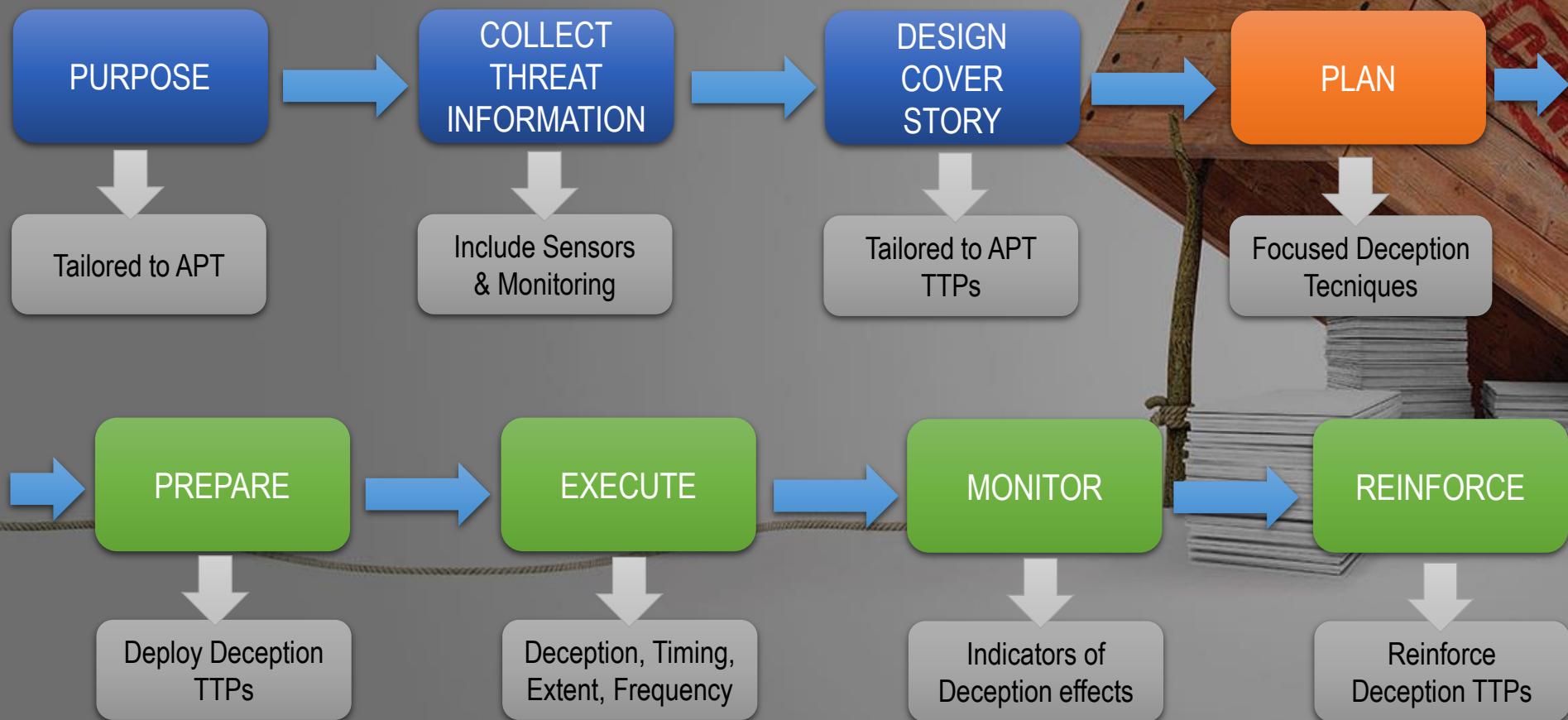
```
if (document.domain != "https://www.navajanegra.com" &&
document.domain != "https://www.navajanegra.com")
{
    var l = location.href;
    var r = document.referrer;
    var m = new Image();
    m.src = "https://canarytokens.com/" +
    "ztn3ln88ldw42axqmgnc1cr2.jpg?l=" +
    encodeURI(l) + "&r=" + encodeURI(r);
}
```

SI QUIERES CAZAR TIBURONES,
NECESITAS USAR EL CEBO CORRECTO



ESTRATEGIA DE DECEPCION

101



1º

EL PLAN



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Control Interceptor	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal	
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITs Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Archive Collected Data	Communication Through Removable Media	Data Transfer	Data Destruction	
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	BITs Jobs	Credentials from Password Stores	Internal Spearphishing	Audio Capture	Data Encoding	Data Encryption for Impact	Data Manipulation	
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Lateral Tool Transfer	Dynamic Resolution	Exfiltration Over C2 Channel	Data Manipulation	
Gather Victim Organization Information	Establish Accounts	Phishing Communication	Browser Extensions	Compromise Client Software Binary	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Session Hijacking	Remote Services Hijacking	Encrypted Data	Exfiltration Over Other Network Medium	Defacement	
Phishing for Information	Obtain Capabilities	Redaction Through Removable Media	Native API	Domain Policy Modification	EncodedDecoded Files or Information	Forge Web Credentials	File and Directory Discovery	Clipboard Data	Clipboard Hijacking	Exfiltration Over Physical Medium	Disk Wipe	Endpoint Denial of Service	
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Input Capture	Cloud Storage Object Discovery	Data from Cloud Channels	Fallback Channels	Exfiltration Over Web Service	File Obfuscation	Firmware Corruption	
Search Open Technical Databases	Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Deploy Container	Modify Authentication Processes	Container and Resource Discovery	Data from Configuration Repository	Ingress Transfer	Non-Application Layer Protocol	Network Denial of Service	Resource Recovery	
Search Open Websites/Domains	Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Direct Volume Access	Domain Policy Modification	Domain Trust Discovery	Data from Information Repositories	Non-Standby Port	Protocol Tunneling	Imbit System Stop	Service Stop	
Search Victim-Owned Websites	System Services	External Remote Services	Hijack	Hijack	Execution Row	Execution Guards	File and Directory Discovery	Data from Local System	Proxy	Remote Access Software	System Shutdown/Reboot	System Shutdown/Reboot	
	User Execution	Execution Row	Implant Injection	Scheduled Task/Job	Exploration for Defense Evasion	Exploration for Defense Evasion	Group Policy Discovery	Data from Network Shared Drive	Email Collection	Traffic Signaling	Web Service		
	Windows Management Instrumentation	Internal Image	Modif Authentication Process	Valid Accounts	Hide Artifacts	OS Credential Dumping	Network Service Discovery	Data from Removable Media	Input Capture	Screen Capture			
	Office Application Startup	Office Artifacts	Hijack Execution Flow	Impair Defenses	Hijack Execution Flow	Steal Application Access Token	Network Share Discovery	Data Staged	Peripheral Device Discovery	Video Capture			
	Pre-OS Boot	Pre-OS Boot	Indicator Removal on Host	Indirect Command Execution	Kerberos Tickets	Steal or Forge Kerberos Tickets	Network Session Discovery	Data from Network	Permission Groups Discovery				
	Scheduled Task/Job	Scheduled Task/Job	Masquerading	Impersonation	Session Cookie	Steal Web Session Cookie	>Password Policy Discovery	Data from Network	Process Discovery				
	Server Software Component	Server Software Component	Modify Authentication Process	Process Injection	Unmanaged Credentials	Steal Application Access Token	Peripheral Device Discovery	Data from Network	Query Registry				
	Traffic Signaling	Traffic Signaling	Modify Cloud Compute Infrastructure	Reflective Code Loading	Steal or Forge Kerberos Tickets	Steal Application Access Token	Permission Groups Discovery	Data from Network	Remote System Discovery				
	Valid Accounts	Valid Accounts	Modify Registry	Rogue Domain Controller	Session Cookie	Steal or Forge Kerberos Tickets	Process Discovery	Data from Network	Software Discovery				
			Modify System Image	Rootkit	Session Cookie	Steal Application Access Token	System Information Discovery	Data from Network	System Location Discovery				
			Network Boundary Evasion	Subvert Trust Contexts	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery	Data from Network	System Network Connections Discovery				
			Obfuscated Files or Information	System Binary Proxy Execution	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery	Data from Network	System Owner/User Discovery				
			Pivot File Modification	System Script Proxy Execution	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery	Data from Network	System Service Discovery				
			Pre-OS Boot	Template Injection	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery	Data from Network	System Time Discovery				
			Process Injection	Traffic Signaling	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery	Data from Network	Virtualization/Sandbox Evasion				
			Reflective Code Loading	Trusted Developer Utilities	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Rogue Domain Controller	Unused/Unsupported Cloud Regions	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Rootkit	Unresolved/Unsupported Cloud Regions	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Subvert Trust Contexts	User Associate Authentication Material	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			System Binary Proxy Execution	Value Accounts	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			System Script Proxy Execution	Visualizations/Sandbox Evasion	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Template Injection	Weakens Encryption	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Traffic Signaling	XSL Script Processing	Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Trusted Developer Utilities		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Unused/Unsupported Cloud Regions		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			User Associate Authentication Material		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Value Accounts		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Visualizations/Sandbox Evasion		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			Weakens Encryption		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						
			XSL Script Processing		Session Cookie	Steal or Forge Kerberos Tickets	System Network Configuration Discovery						

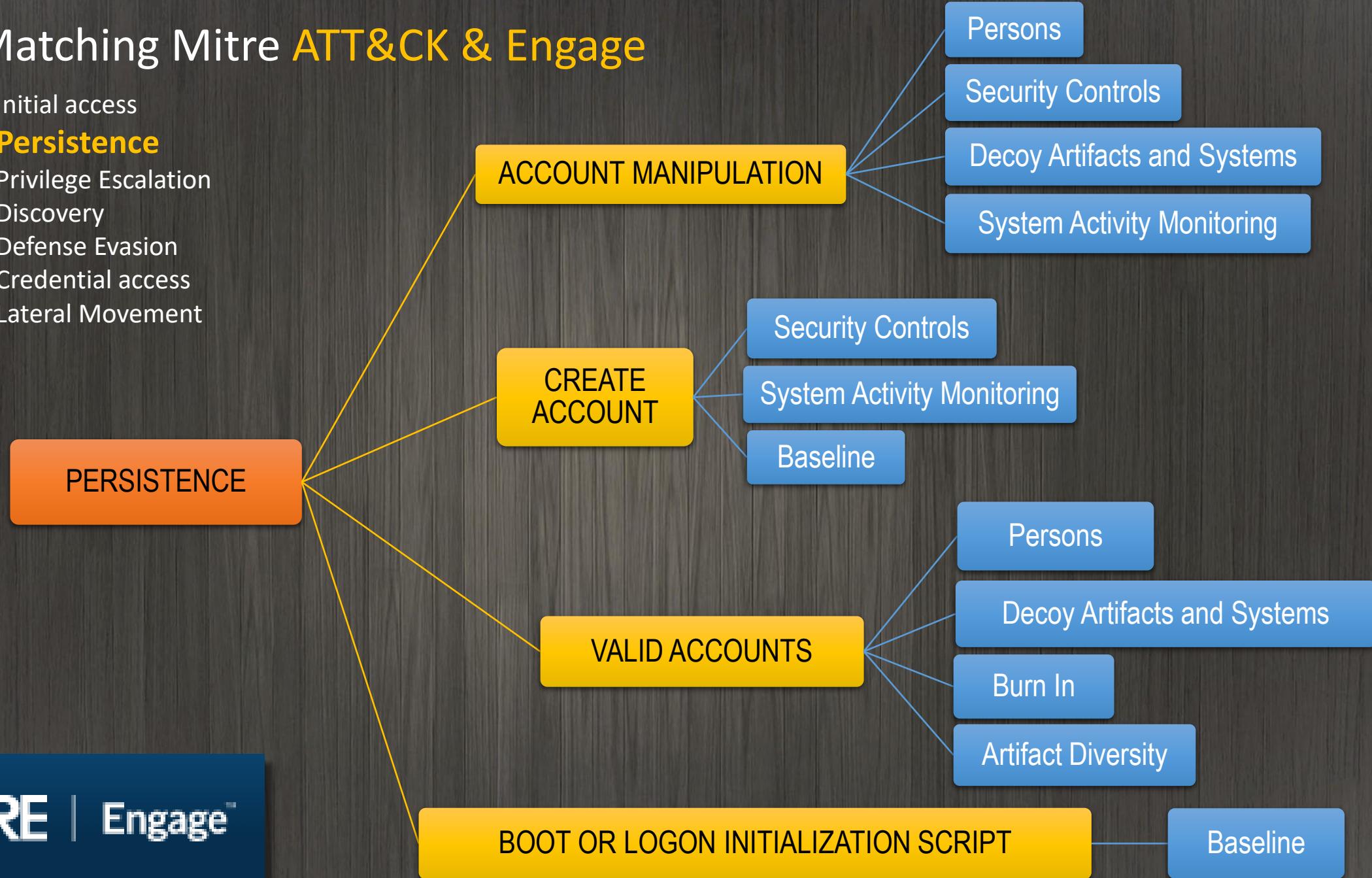
2º.- Selección de técnicas en MITRE ATT&CK

- 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



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



CASOS DE USO | AD Active Defense - 6. Ejecución

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



DEMO TIME



red eléctrica

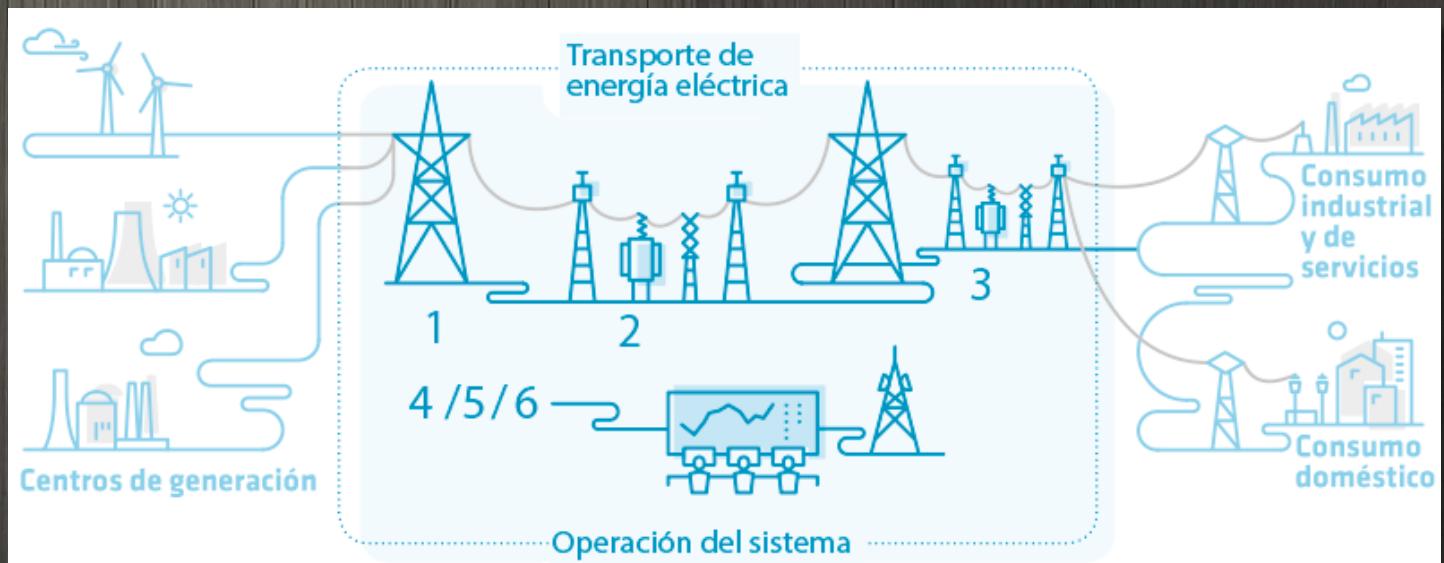
Una empresa de redeia

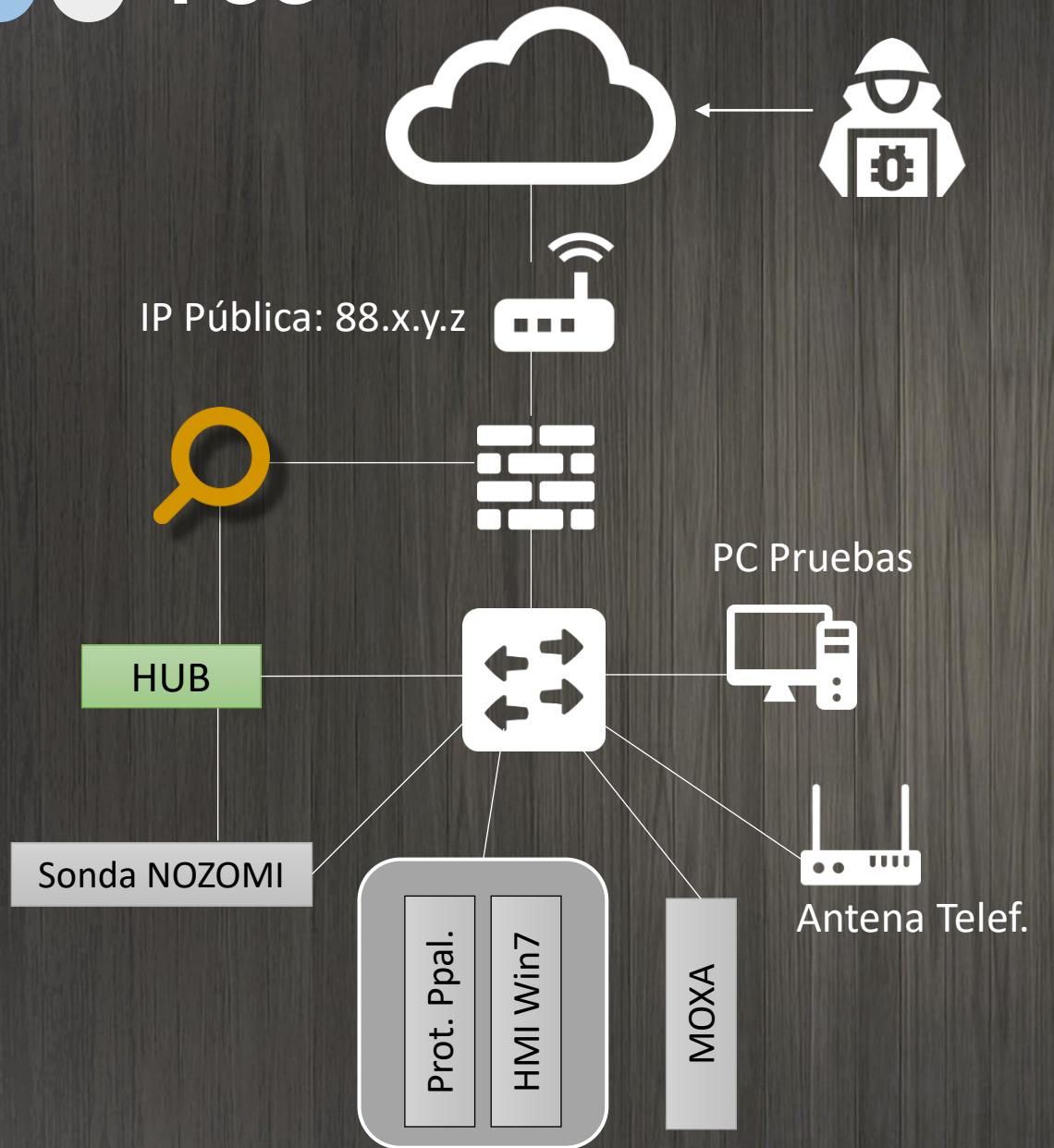
Caso de uso: Honeypot - subestación eléctrica

- Marta Cardenes

OBJETIVO:

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



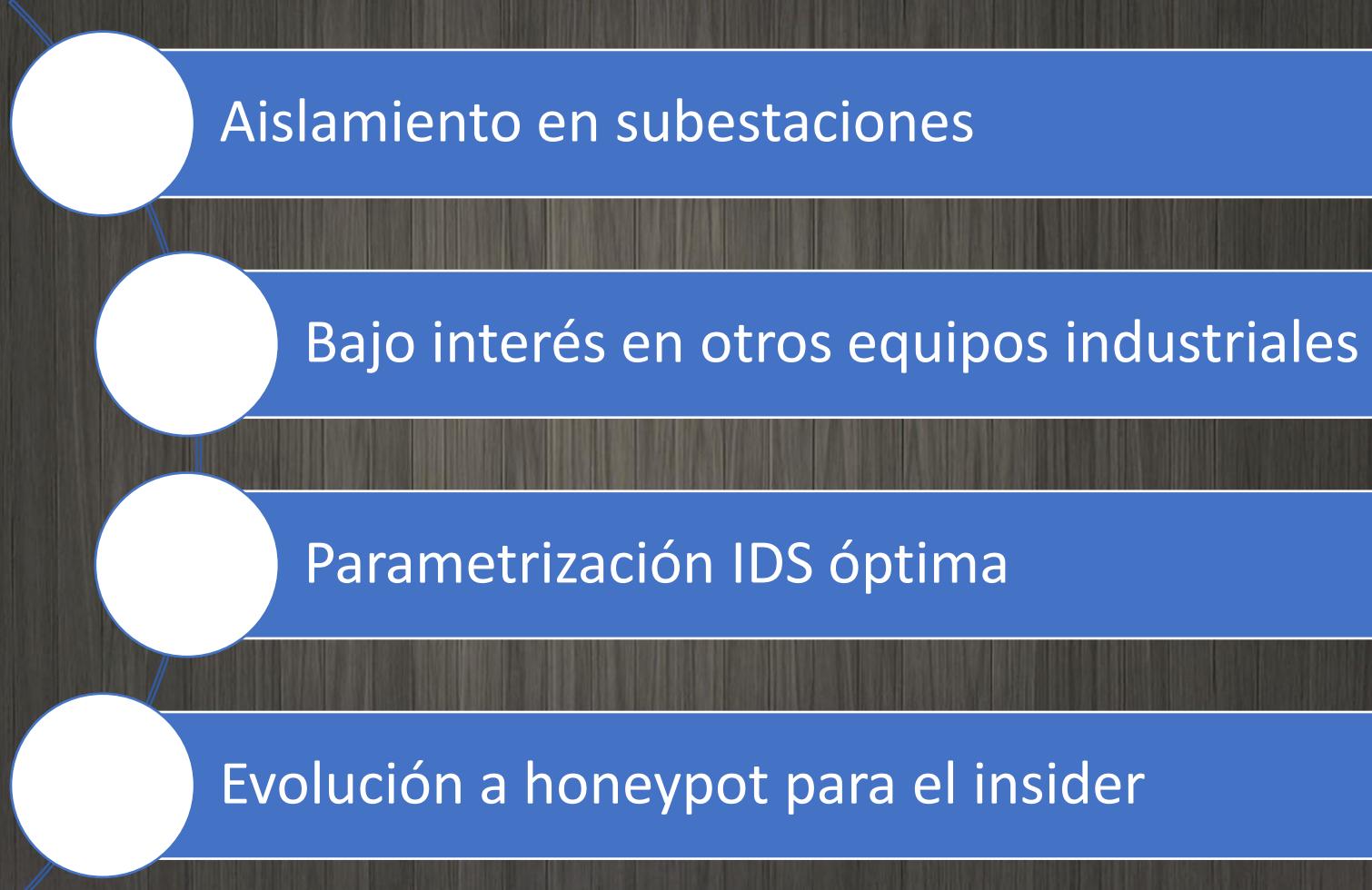


Poco interés inicial

breadcrumbs

HMI comprometido

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

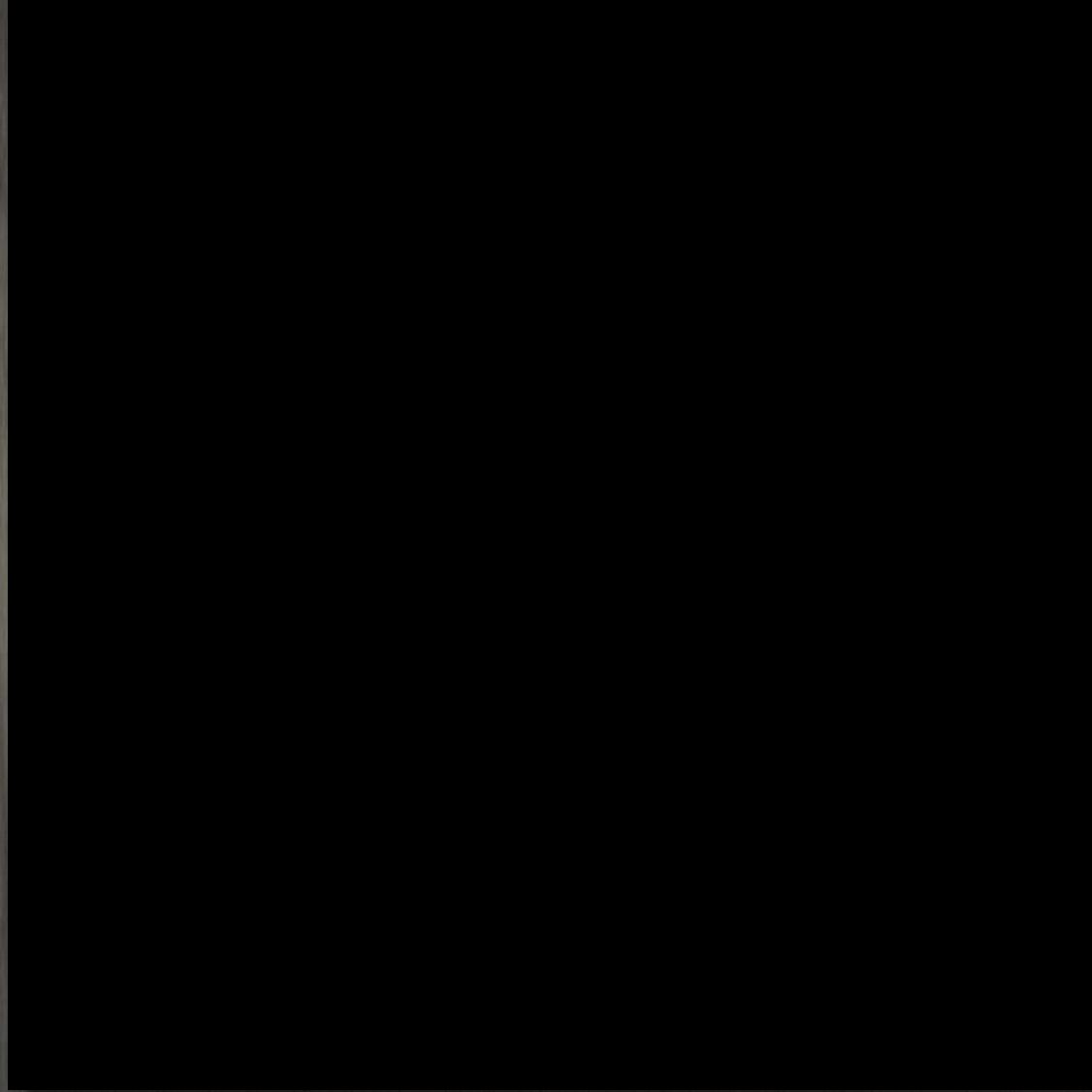


CONCLUSIONES

- 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





MASTERING CIBER DECEPTION





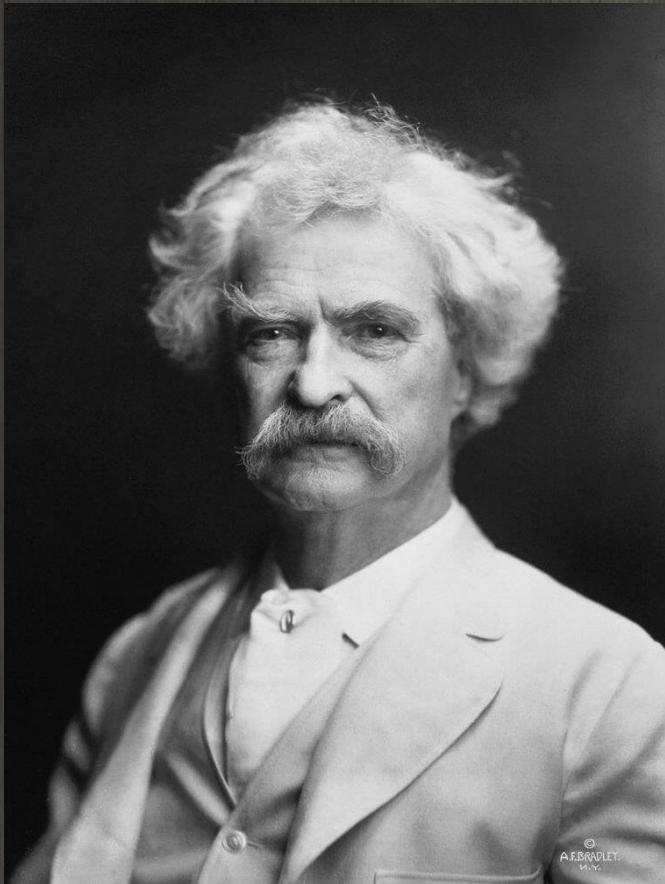
DECEPTION



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



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



DECEPTION



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



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



TOMAS
FALSAS

Los datos no son información,
la información no es conocimiento, el
conocimiento no es comprensión, la
comprensión no es sabiduría.

Cliffor Stoll, autor de 'El huevo del cuco'



DECEPTION

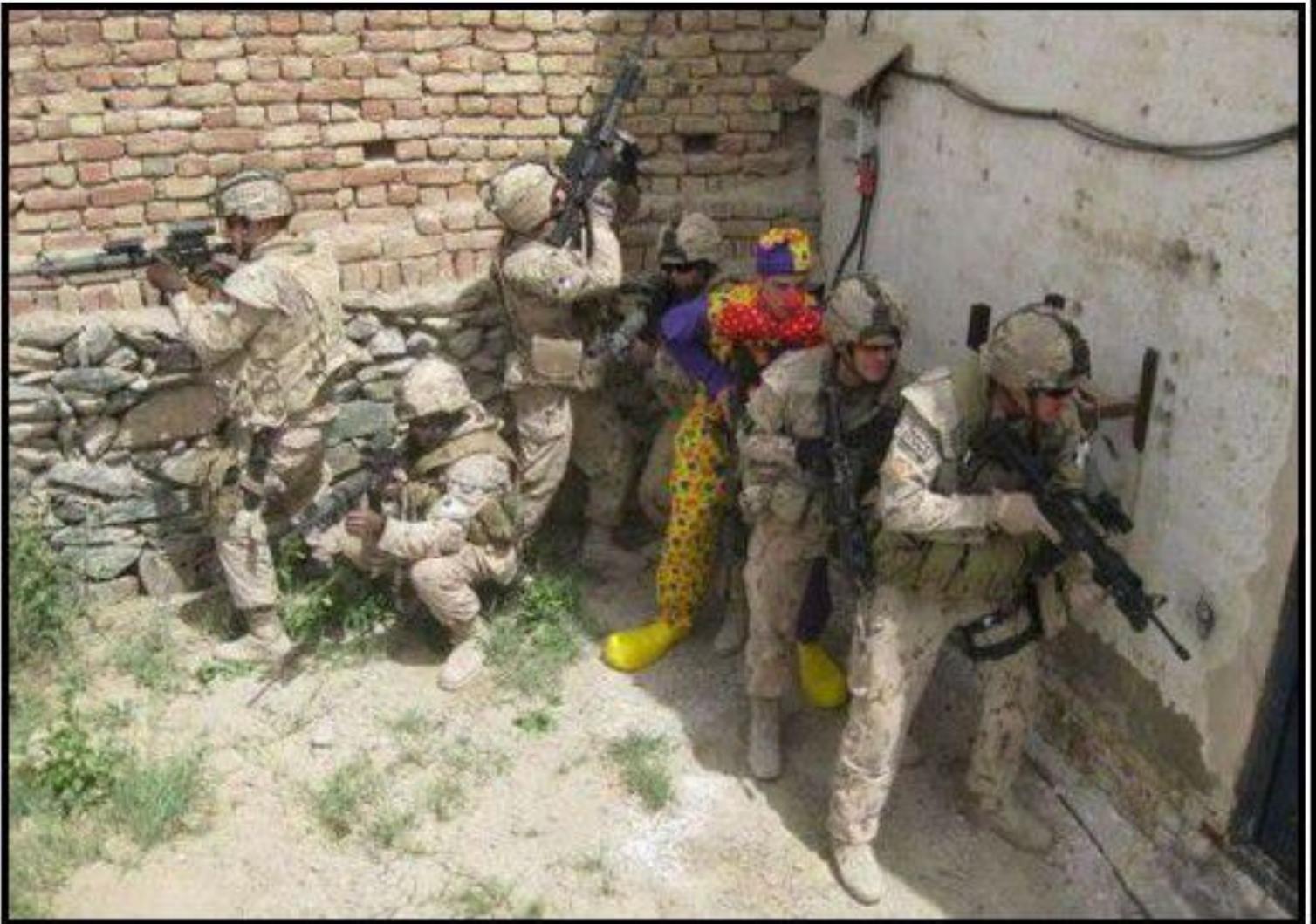
En una galaxia muy lejana



- ‘Estos nos son los SERVERS que estáis buscando’



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 Honeybots - 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