Digital Security
Progress. Protected.

EVENTO PRESENCIAL

Inteligencia Artificial convertida en ataque:

¿Cómo los hackers pueden usar la IA en tu contra?

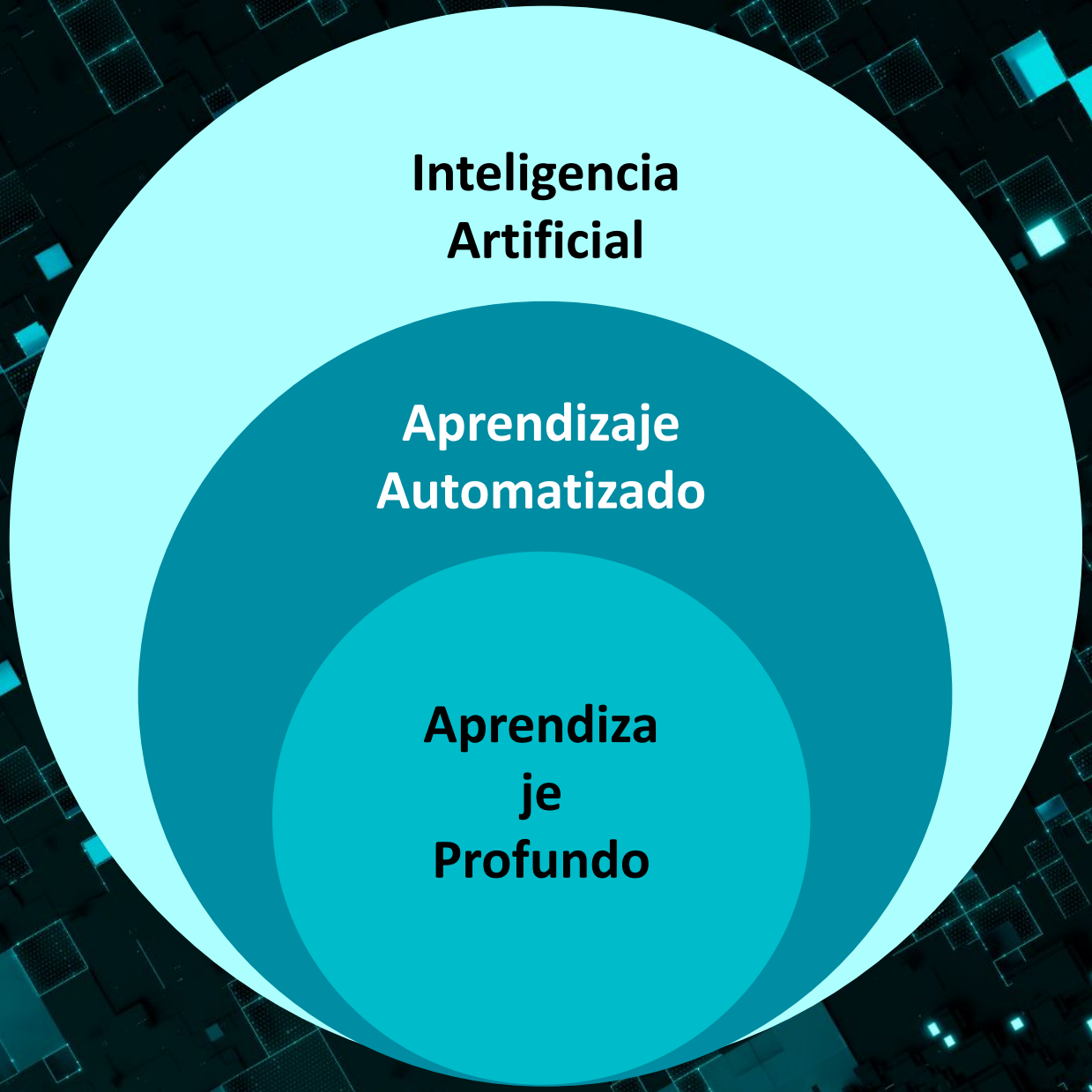
Digital Security
Progress. Protected.

Inteligencia Artificial Ofensiva

Fátima Rodríguez – Cybersecurity Intelligence Analyst

“A computer would deserve to be called intelligent if it could deceive a human into believing that it was human.”

— Alan Turing



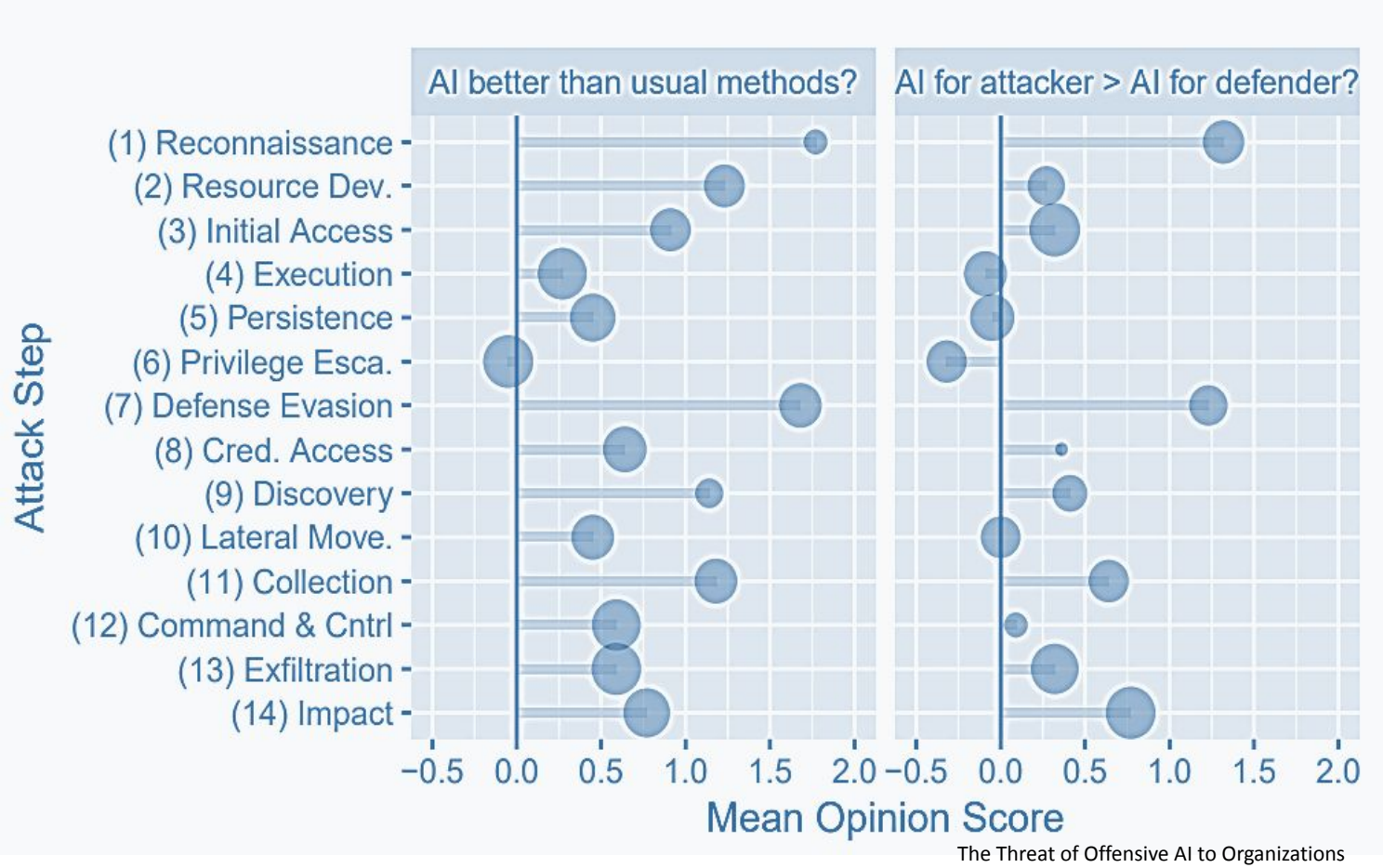
Incorporar comportamiento humano inteligente

Aprende y mejora automáticamente de la experiencia*

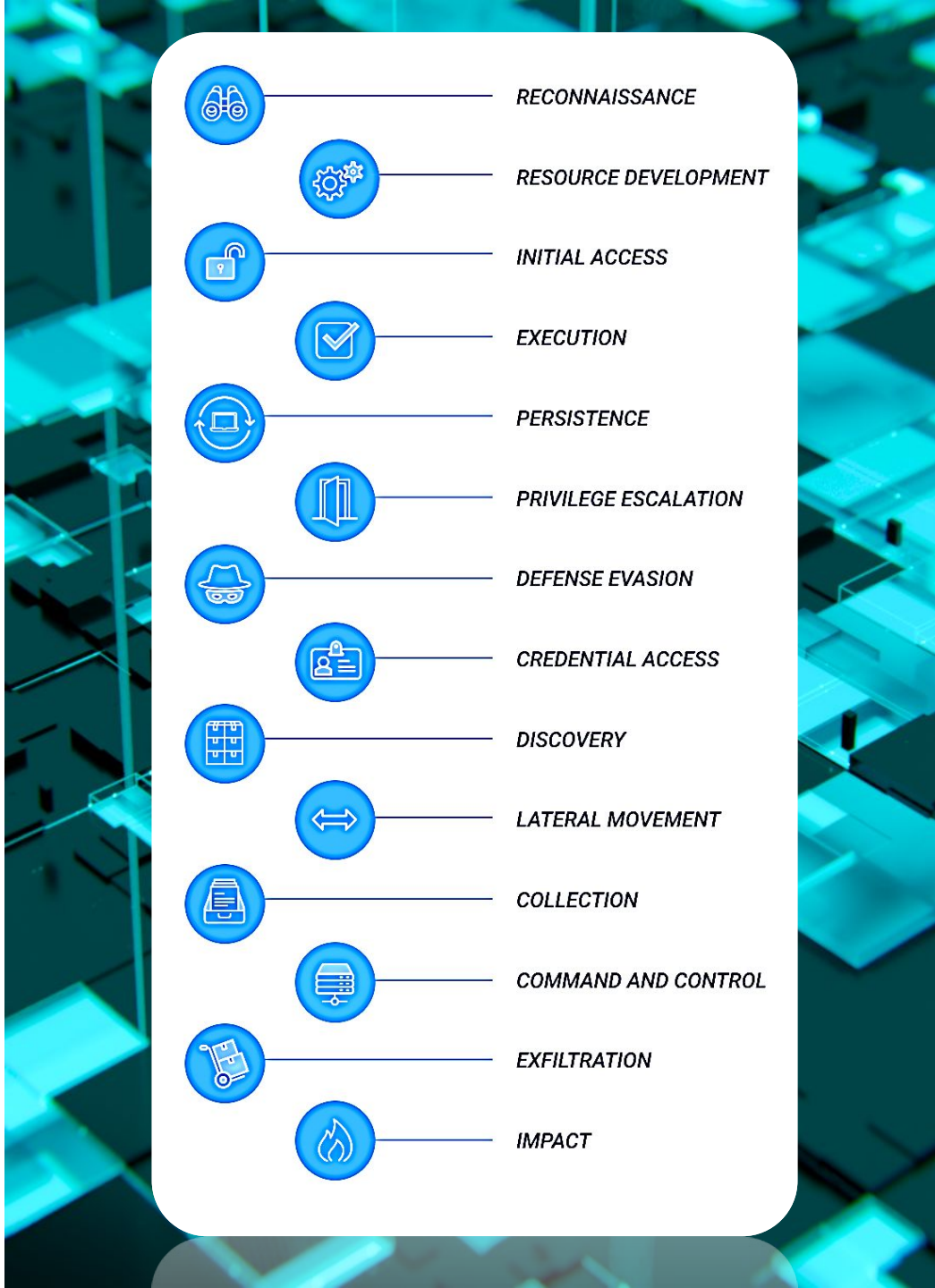
Utiliza algoritmos complejos y redes neuronales para entrenar un modelo.

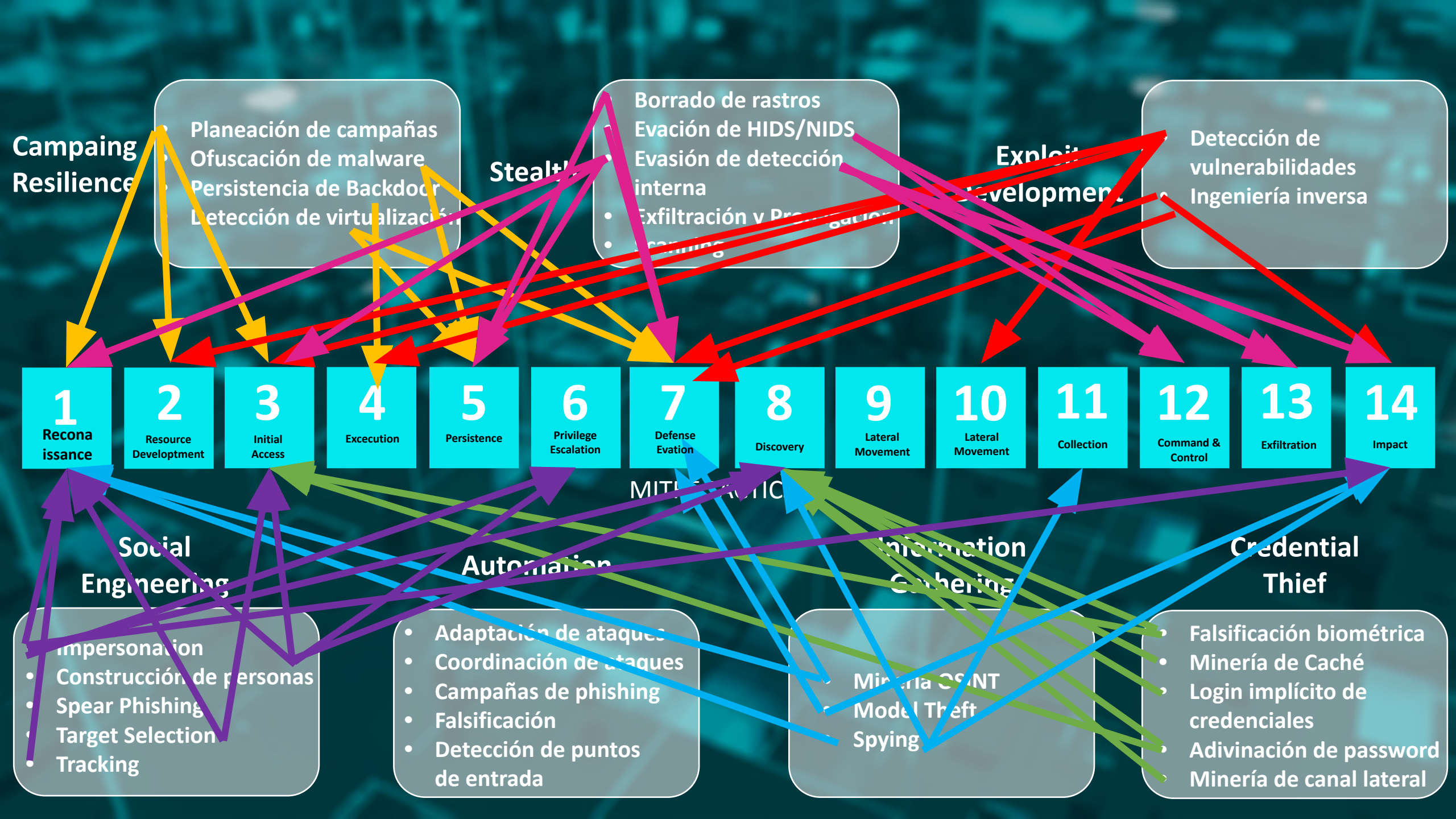
Panorama de la Industria

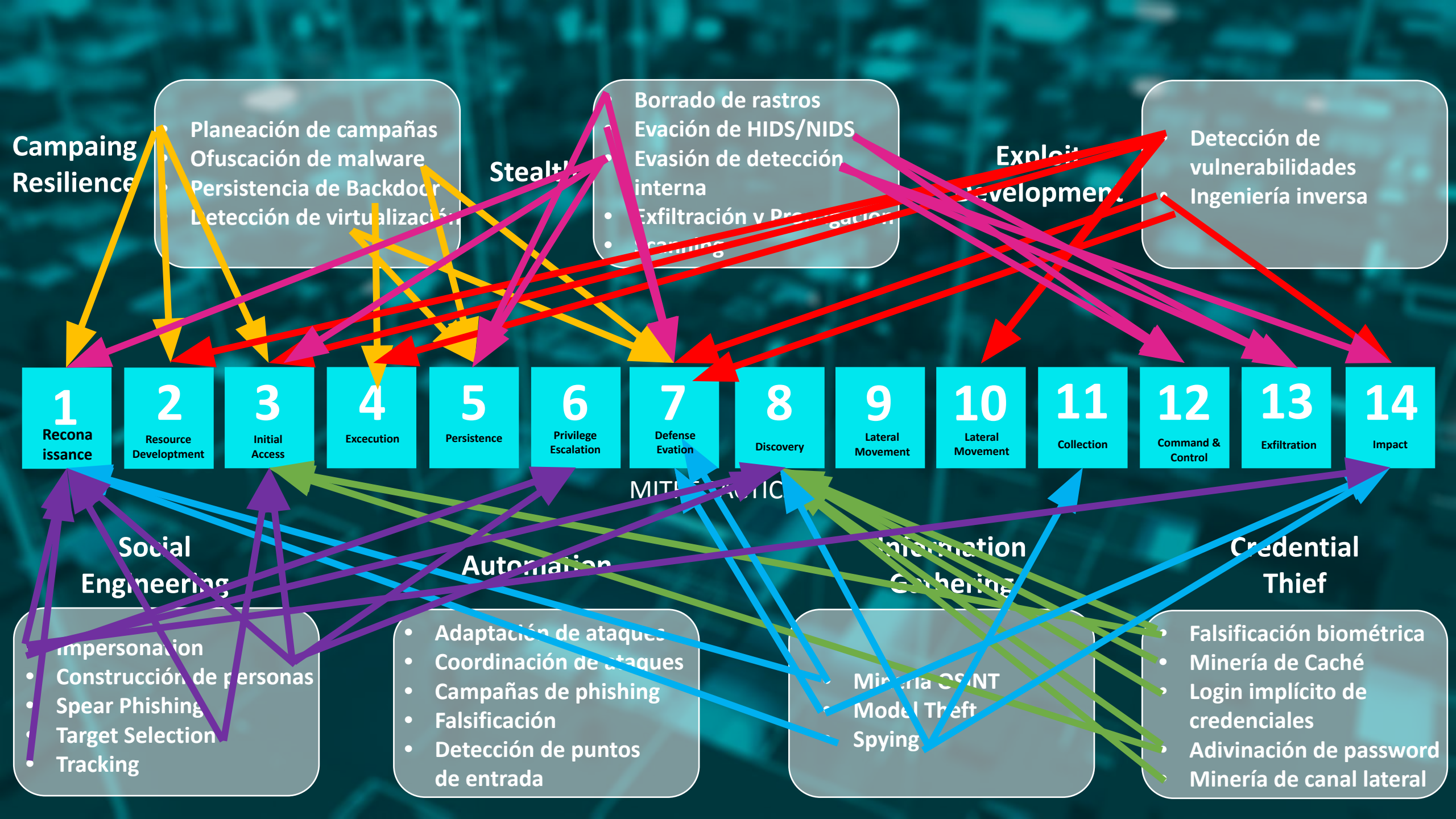
Percepción del uso de la Inteligencia Artificial en ciberataques



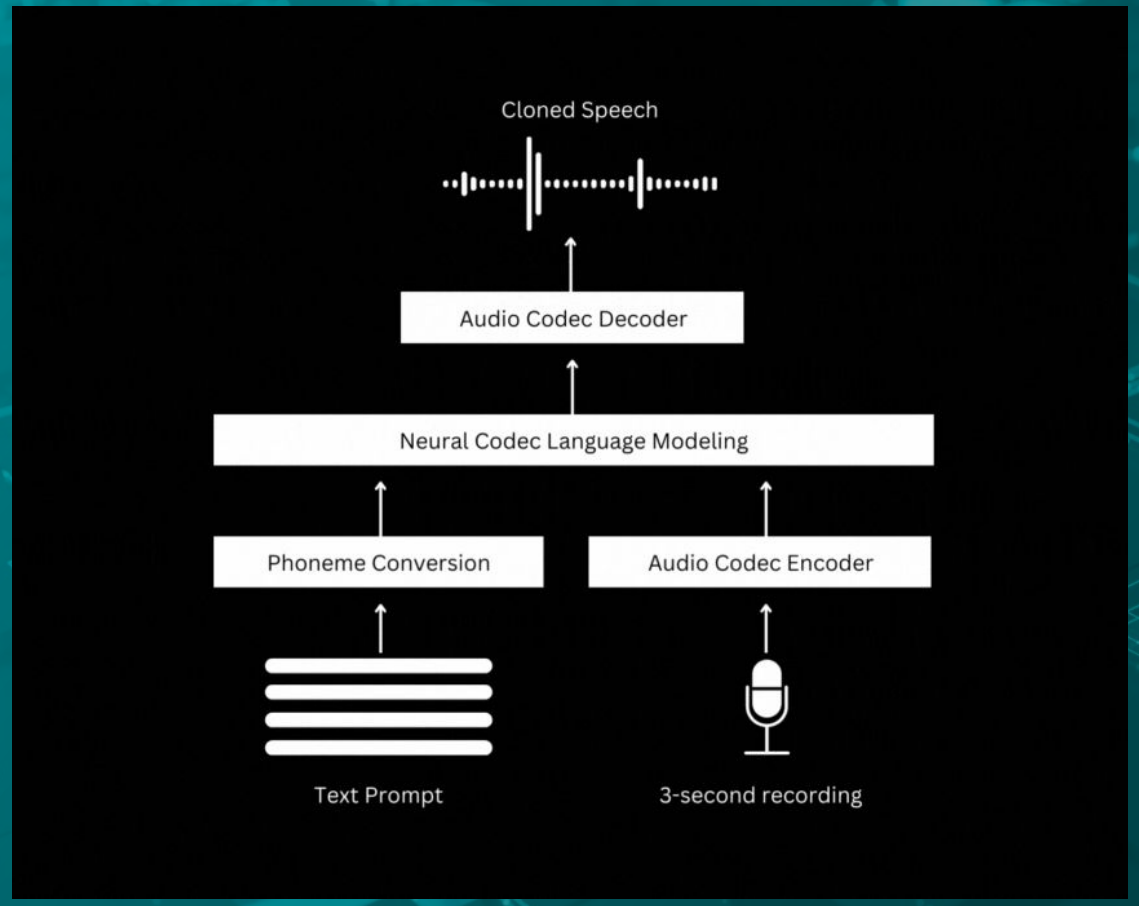
The Threat of Offensive AI to Organizations

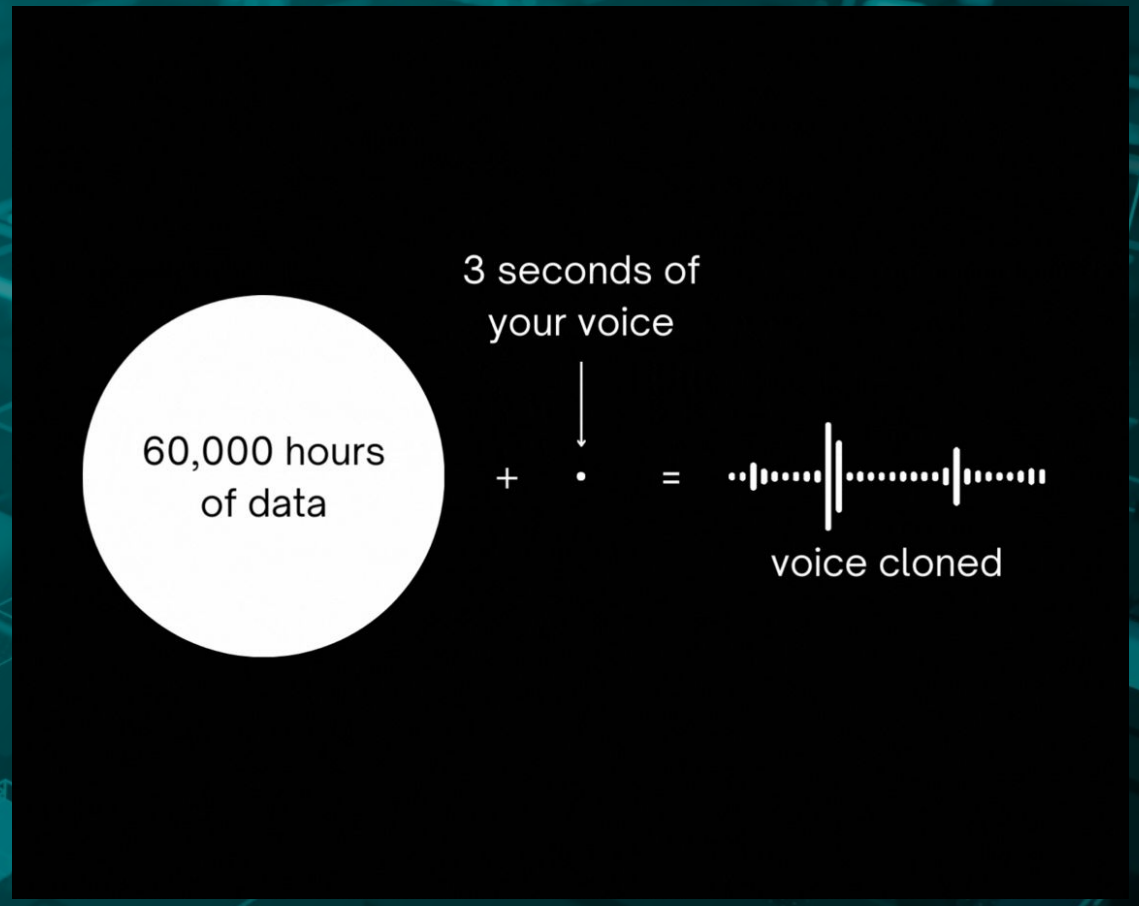



Campaing
Resilience
Planeación de campañas
Ofuscación de malware
Persistencia de Backdoor
Detección de virtualizaci
Stealth
Borrado de rastros
Evación de HIDS/NIDS
Evasión de detección interna
Exfiltración y Pr
Exploit
evelopment
Detección de vulnerabilidades
Ingeniería inversa
1 Recona issance
2 Resource Developtment
3 Initial Access
4 Excecution
5 Persistence
6 Privilege Escalation
7 Defense Evation
8 Discovery
9 Lateral Movement
10 Lateral Movement
11 Collection
12 Command & Control
13 Exfiltration
14 Impact
MITRE ATTACK
Social Engineering
mpersonation
Construcción de personas
Spear Phishing
Target Selection
Tracking
Automation
Adaptación de ataques
Coordinación de ataques
Campañas de phishing
Falsificación
Detección de puntos de entrada
Information Gathering
Minería OSINT
Model Theft
Spying
Credential Thief
Falsificación biométrica
Minería de Caché
Login implícito de credenciales
Adivinación de password
Minería de canal lateral


Campaing
Resilience
Planeación de campañas
Ofuscación de malware
Persistencia de Backdoor
Detección de virtualizaci
Stealth
Borrado de rastros
Evación de HIDS/NIDS
Evasión de detección interna
Exfiltración y Pr
Exploit
evelopment
Detección de vulnerabilidades
Ingeniería inversa
1 Recona issance
2 Resource Developtment
3 Initial Access
4 Excecution
5 Persistence
6 Privilege Escalation
7 Defense Evation
8 Discovery
9 Lateral Movement
10 Lateral Movement
11 Collection
12 Command & Control
13 Exfiltration
14 Impact
MITRE ATTACK
Social Engineering
mpersonation
Construcción de personas
Spear Phishing
Target Selection
Tracking
Automation
Adaptación de ataques
Coordinación de ataques
Campañas de phishing
Falsificación
Detección de puntos de entrada
Information Gathering
Minería OSINT
Model Theft
Spying
Credential Thief
Falsificación biométrica
Minería de Caché
Login implícito de credenciales
Adivinación de password
Minería de canal lateral

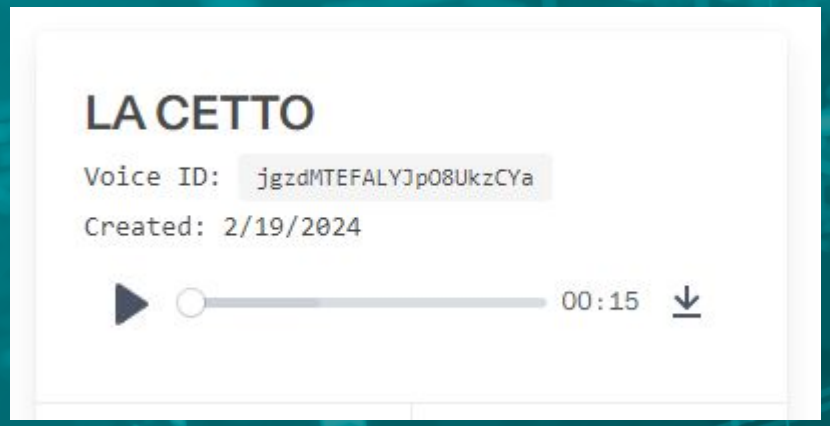
Social Engineering





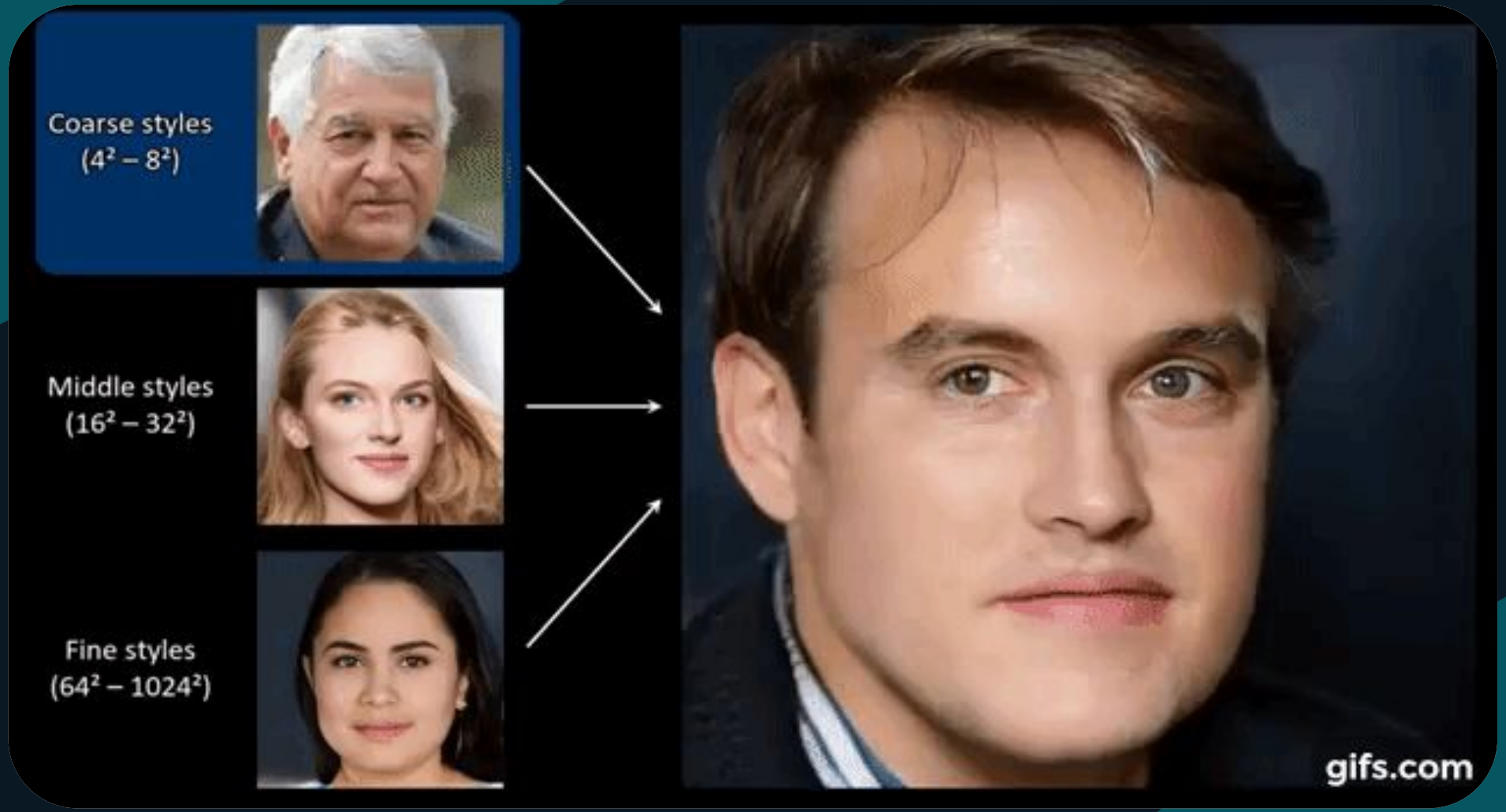
IMPERSONATION

IMPERSONATION



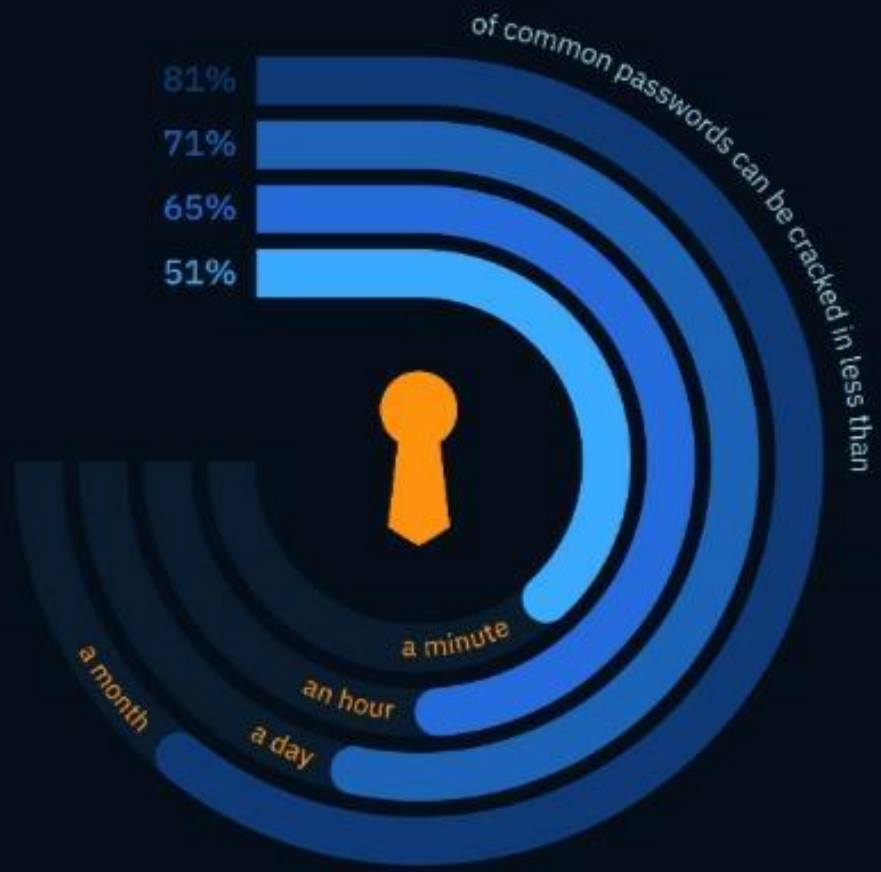
Credential Thief

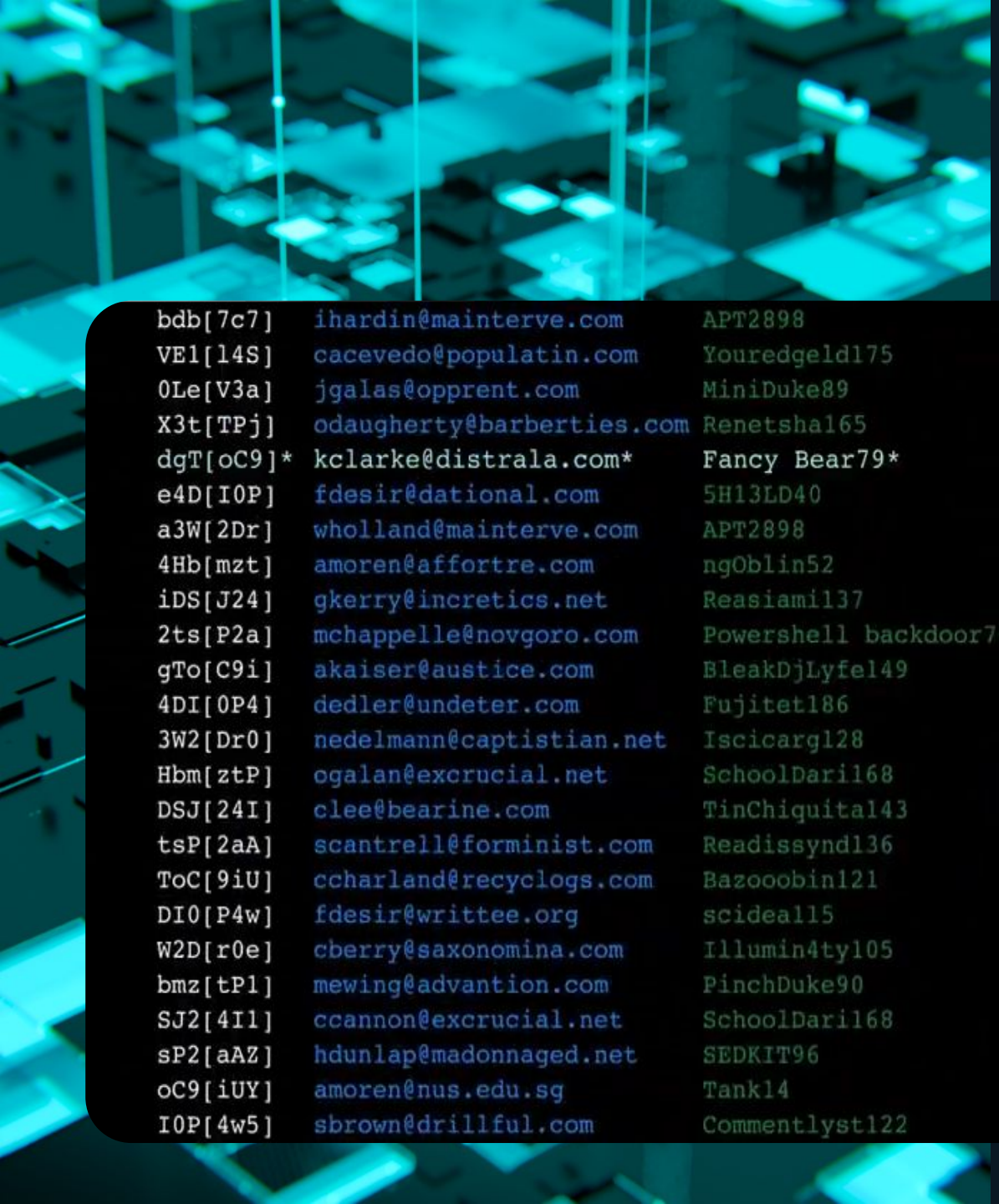
PASSWORD GUESSING



PASSWORD GUESSING

51%	of common passwords can be cracked in less than	a min
65%	of common passwords can be cracked in less than	an hour
71%	of common passwords can be cracked in less than	a day
81%	of common passwords can be cracked in less than	a month





PASSWORD GUESSING

bdb[7c7]	ihardin@mainterve.com	APT2898	nnpN@p?y#j	113.89.216.98	73.41.b7.d0.0f.13	14:47
VE1[l4S]	cacevedo@populatin.com	Youredgeld175	f>?AL?nhzKH	89.216.98.246	53.c8.b4.63.6a.43	13:40
0Le[V3a]	jgalas@opprent.com	MiniDuke89	<s,%gffota	216.98.246.95	d6.a8.0b.42.0c.40	19:40
X3t[TPj]	odaugherty@barberties.com	Renetsha165	i%WIY2b!?YRo	98.246.95.122	62.4d.3b.83.ee.ca	14:05
dgT[oC9]*	kclarke@distrala.com*	Fancy Bear79*	qbDxih.*	121.124.109.233*	75.33.c2.ae.8e.d2*	15:12*
e4D[I0P]	fdesir@dational.com	5H13LD40	rF<?/,LXf>	124.109.233.144	76.04.0c.42.31.da	15:21
a3W[2Dr]	wholland@mainterve.com	APT2898	mgE<&#)v<	109.233.144.222	62.a2.aa.3b.34.d2	14:38
4Hb[mzt]	amoren@affortre.com	ngOblin52	?o[WKD?	233.144.222.132	ee.48.0e.fd.d7.78	20:28
iDS[J24]	gkerry@incretics.net	Reasiami137	yb;LmRt	144.222.132.234	9c.a5.b3.b0.91.fc	16:16
2ts[P2a]	mchappelle@novgoro.com	Powershell backdoor70	;#:BORKi	222.132.234.229	d0.52.bd.c7.fb.da	19:57
gTo[C9i]	akaiser@austice.com	BleakDjLyfe149	u6?dmvr%r??	132.234.229.32	83.d3.c5.6b.e2.15	15:41
4DI[0P4]	dedler@undeter.com	Fujitet186	?MW(s?f,	234.229.32.14	ee.9f.e2.a7.2e.41	20:31
3W2[Dr0]	nedelmann@captistian.net	Iscicarg128	,:@s98*,	229.32.14.186	ef.3b.4e.0b.7c.2d	20:17
Hbm[ztP]	ogalan@excrucial.net	SchoolDari168	L4%>#,Fz	32.14.186.79	1d.0d.13.96.3e.d6	10:59
DSJ[24I]	clee@bearine.com	TinChiquita143	FO?;ru?W?	14.186.79.15	07.11.e5.56.8e.13	10:10
tsP[2aA]	scantrell@forminist.com	Readissynd136	$Wllskx&	186.79.15.91	b2.81.65.b2.00.0c	18:15
ToC[9iU]	ccharland@recyclogs.com	Bazooobin121	bDxih.wn	79.15.91.115	45.79.1d.fe.6f.4f	13:13
DI0[P4w]	fdesir@writtee.org	scidea115	F<?/,LXf>?AL	15.91.115.78	04.36.d1.b5.ba.7b	10:11
W2D[r0e]	cberry@saxonomina.com	Illumin4ty105	gE<&#)	91.115.78.184	56.df.31.ee.dd.3e	13:46
bmz[tP1]	mewing@advantion.com	PinchDuke90	o[WKD?Yi%	115.78.184.166	7a.59.29.74.7b.ad	14:53
SJ2[4I1]	ccannon@excrucial.net	SchoolDari168	b;LmRts?	78.184.166.36	4e.77.a0.32.95.77	13:09
sP2[aAZ]	hdunlap@madonnaged.net	SEDKIT96	#:BORKih	184.166.36.225	bf.f6.c5.94.92.8c	18:09
oC9[iUY]	amoren@nus.edu.sg	Tank14	6?dmvr%r??I	166.36.225.159	a3.dd.6c.3f.aa.7e	17:18
I0P[4w5]	sbrown@drillful.com	Commentlyst122	MW(s?f,G	36.225.159.41	2f.af.bc.24.1b.df	11:10

IMPACTO DE LA IA OFENSIVA

¿Por qué es importante?

Entender la Motivación

- ¿Cuáles son los posibles impactos sociales de los ciberataques impulsados por la IA?
- ¿Qué marco se puede utilizar para comprender los ciberataques impulsados por la IA?
- ¿Qué estrategias y técnicas se pueden utilizar para mitigar los ciberataques impulsados por la IA?

¿Cómo pueden ayudar los servicios de Ethical Hacking?

INGENIERÍA SOCIAL

PENTESTING

The Zeroth Law: “A robot may not harm humanity, or, by inaction, allow humanity to come to harm.”

— Isaac Asimov, I, Robot

Digital Security
Progress. Protected.

EVENTO PRESENCIAL

Inteligencia Artificial convertida en ataque:

¿Cómo los hackers pueden usar la IA en tu contra?

GRACIAS