fluid attacks
we hack your software

Más allá de la regulación: Desarrollo ágil y seguro

CELAES 2023

Masoquismo y exhibicionismo: Matando el cáncer asintomático del CISO

Rafael Álvarez (ralvarez@fluidattacks.com)

CELAES 2023

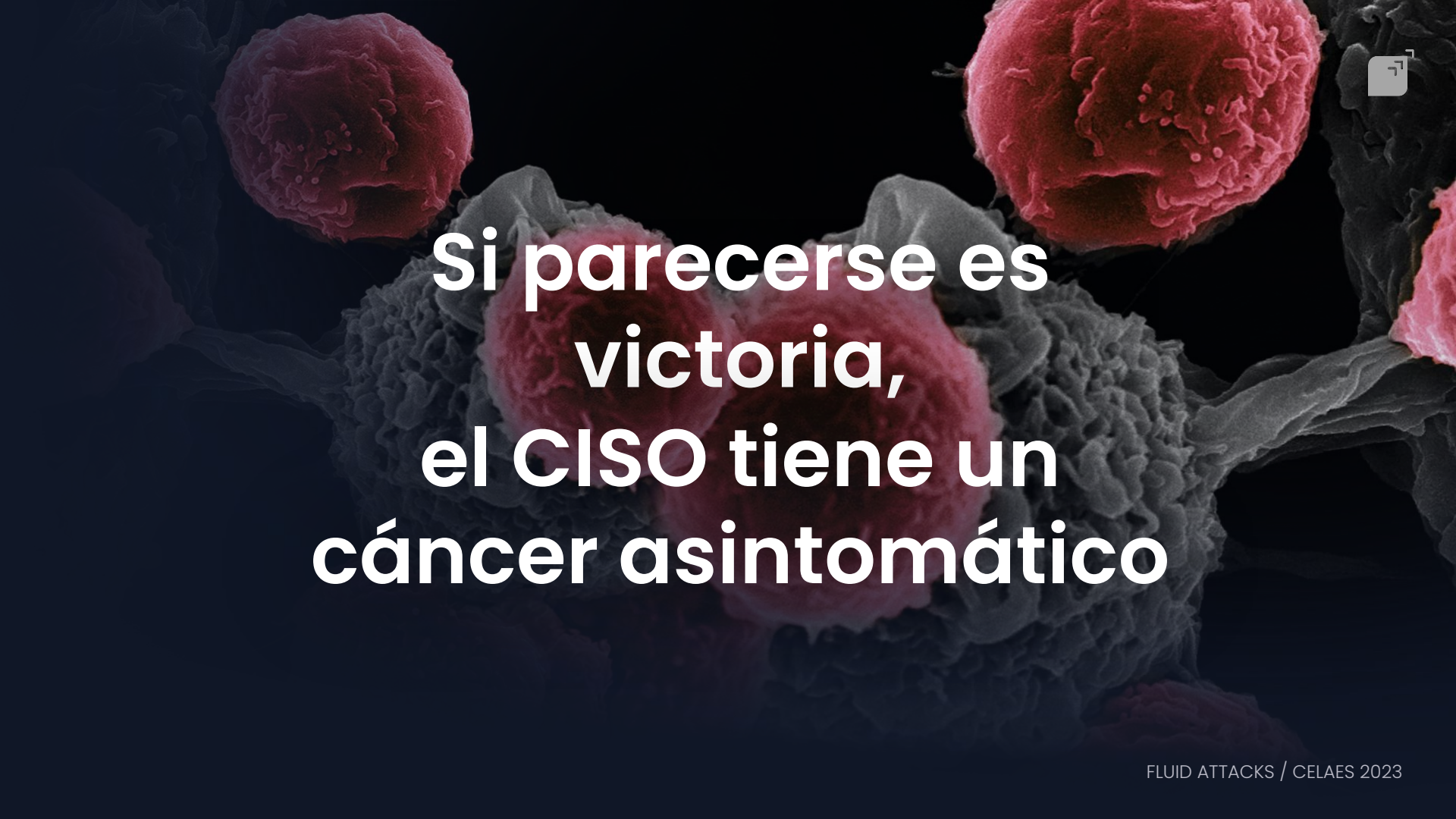
PROBLEMA

¿Qué es ganar para un CISO?

¿Cuál es la definición de victoria?

1. ¿Ejecutar el plan de compra de remedios?
2. ¿Pasar las auditorías de reguladores/proveedores?
3. ¿Estar certificado (ISO27K, SOC2)?
4. ¿El % de cumplimiento de un modelo?
5. ¿Parecerse en los “cómos” a otros referentes?
6. ¿*Value-at-risk* en el tiempo?
7. ¿Parecerse a lo que dicen las consultoras?
8. ¿No terminar en la cárcel?

Solo comparamos
CÓMOS,
no **RESULTADOS**



Si parecerse es victoria, el CISO tiene un cáncer asintomático

CAUSA

Seguimos pensando en remedios

- **Virus,** ahora ***malware***
- **Antivirus,** ahora **XDR**
- **IDS,** ahora **SOC**
- **IPS,** ahora **SOAR**
- **VPNs,** ahora **ZTNA**

Mismas funciones, otros nombres

… y en remedios "estratégicos"

"Necesitamos cultura"

"Eduquemos al usuario"

"Alineémonos a la estrategia"

monos a la ategia"

"¡Hablémosle a la alta dirección!"

"Cooperemos, porque es un problema de todos"

"Ne

O ¿no lo estamos logrando?

O ¿no es lo que tenemos que hacer?

La paradoja de la preparación

Cuando se invierte para construir un edificio o un puente:

1. El logro es **visible**
2. Su **existencia** determina el éxito
3. El resultado rompe el **silencio**

Pero, cuando invertimos en atributos como seguridad o protección:

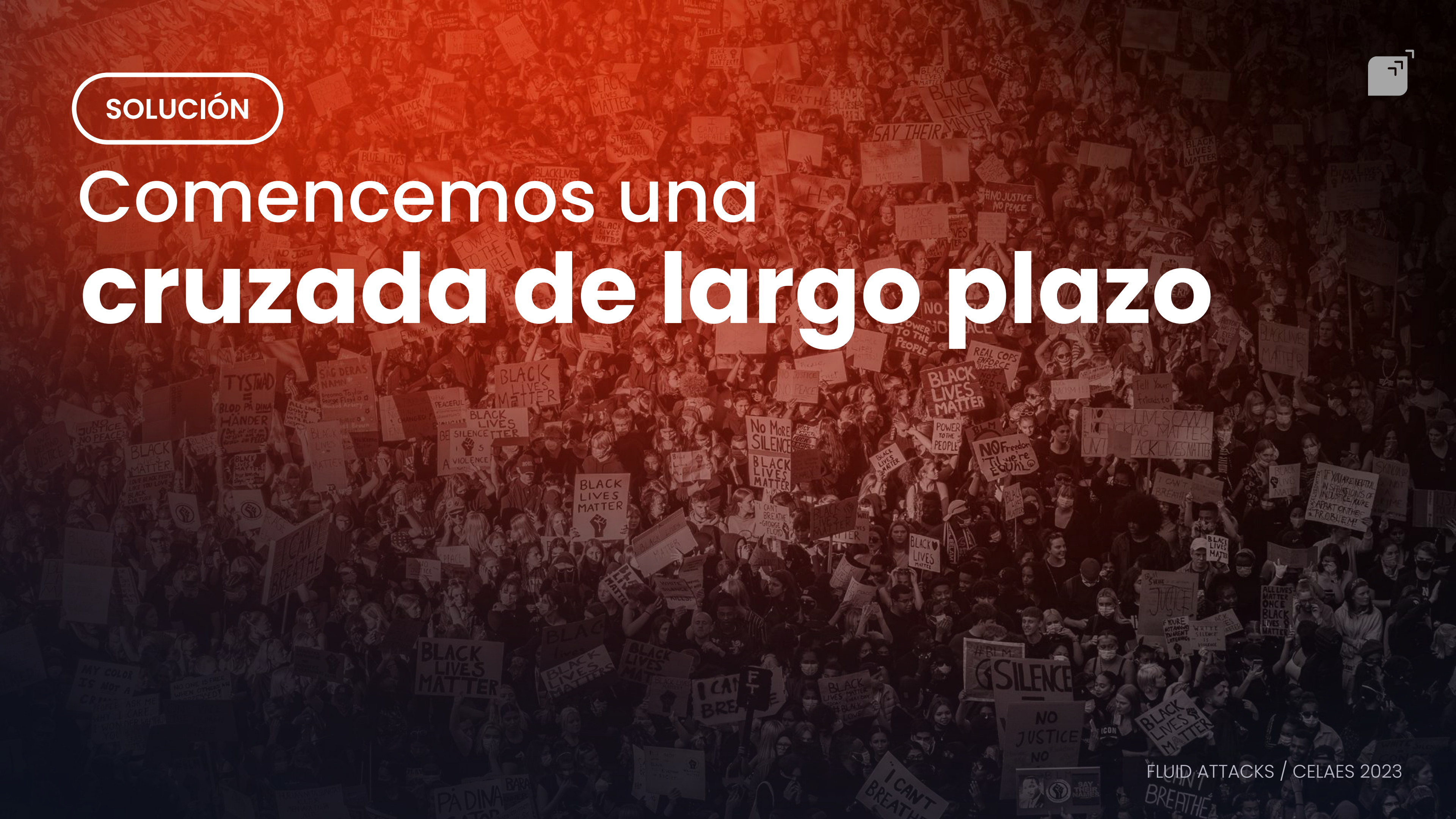
1. El logro es **invisible**
2. La **inexistencia** determina el éxito
3. El resultado es **el silencio**

Por ende, si no pasa nada, surgen las siguientes preguntas:

- ¿Lo logré?
- ¿Tuve suerte?
- ¿Invertí más de la cuenta?

SOLUCIÓN

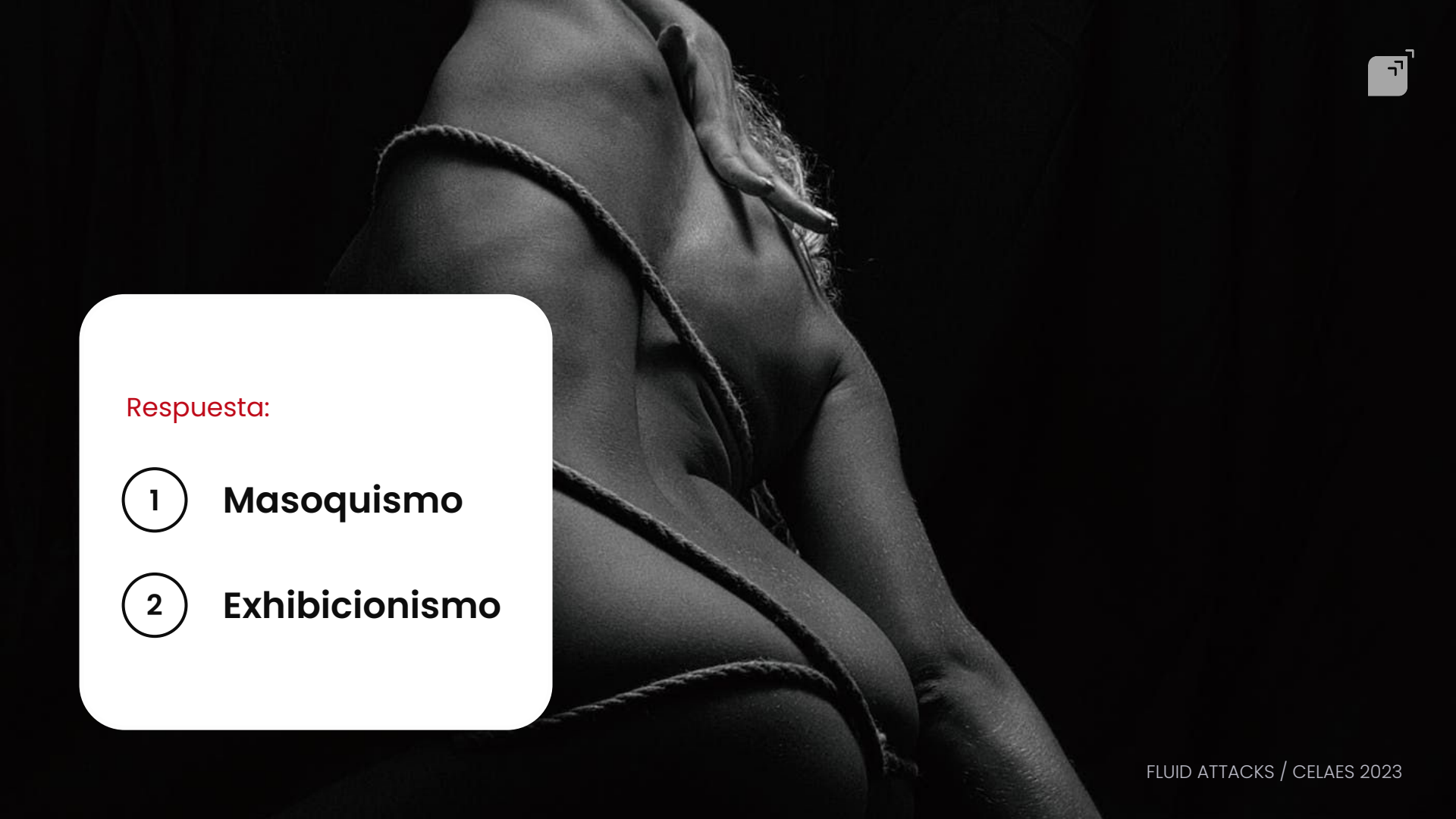
Comencemos una **cruzada de largo plazo**



¡Si yo fuera el regulador!
¡Si yo fuera un CISO dictador!

Que aplicados, **cambien consistentemente** lo demás.

Feedback organizacional. Aprendizaje.

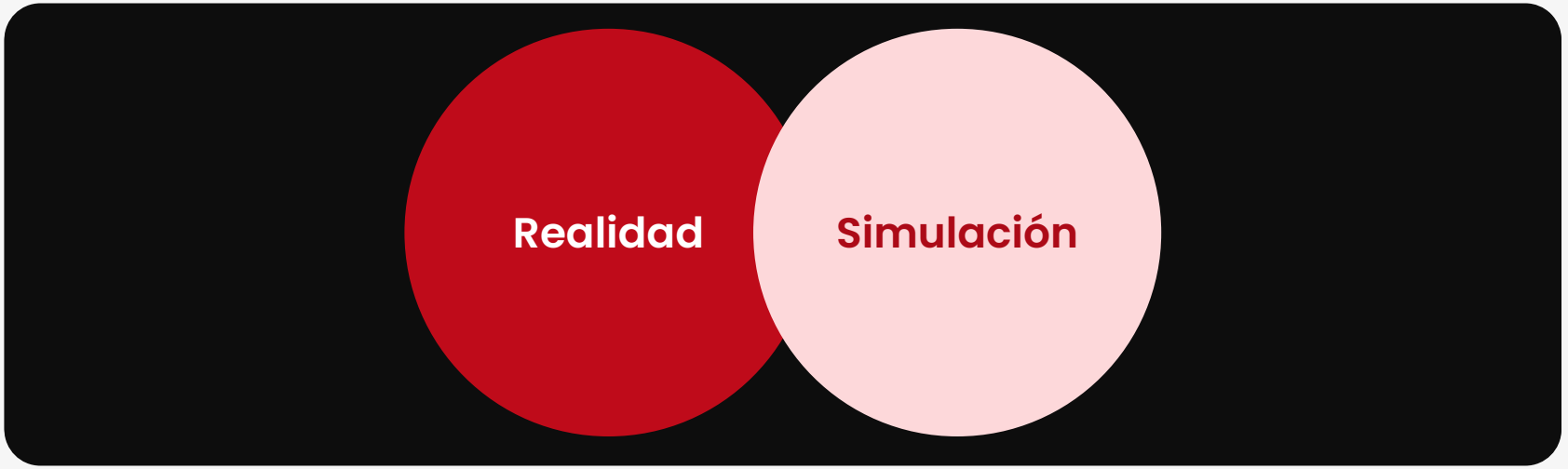


Respuesta:

1. **Masoquismo**
2. **Exhibicionismo**

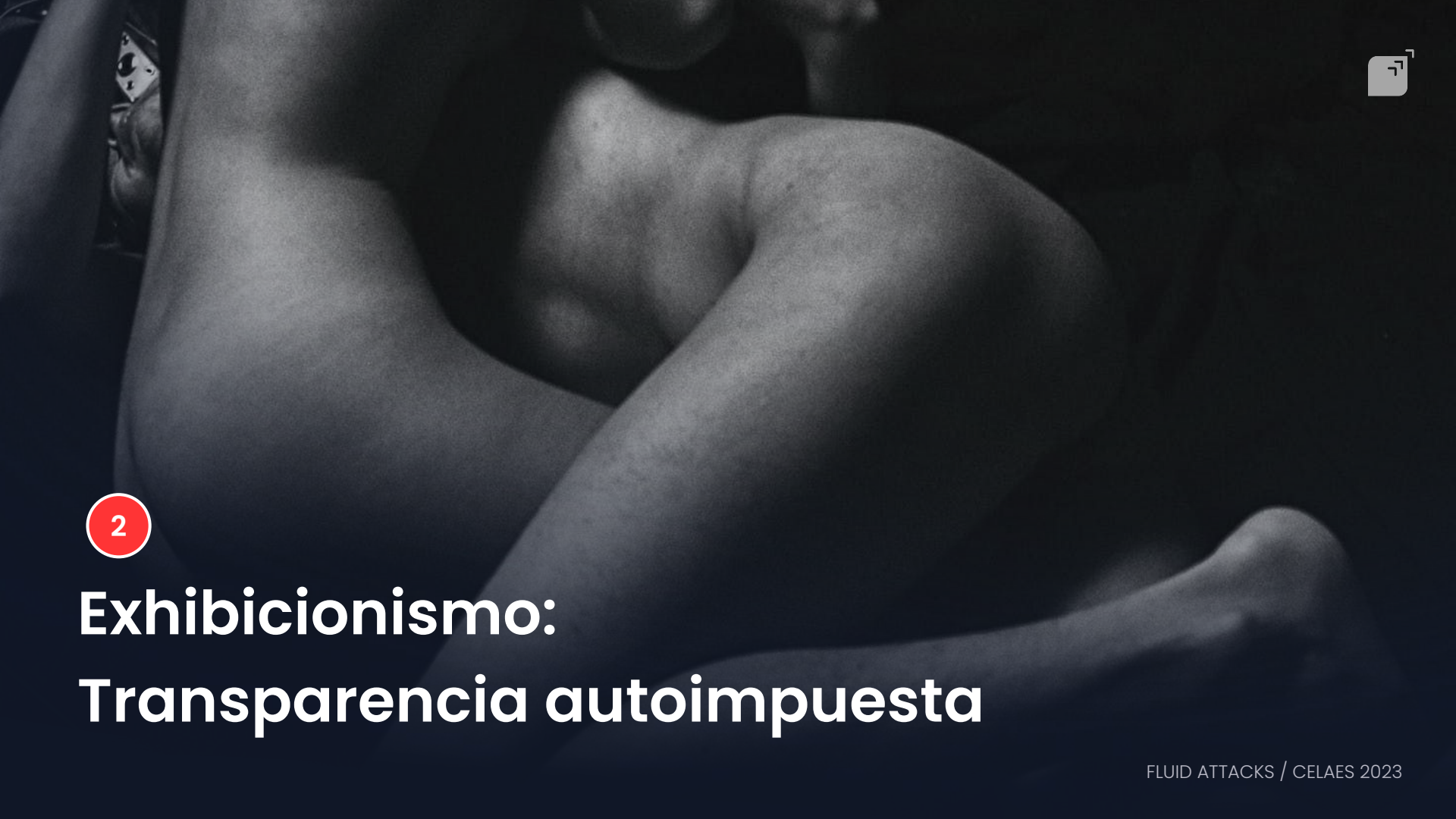
1

Masoquismo: Simulaciones realistas



Causarme incidentes consistentemente:

- Ataques de cero conocimiento
- Ataques sin parar
- Reaccionar hasta el final
- Proporcionalidad
- Coherencia



2

Exhibicionismo: Transparencia autoimpuesta

Publicar al mundo:

Disponibilidad

Rendimiento

Código fuente

Incidentes

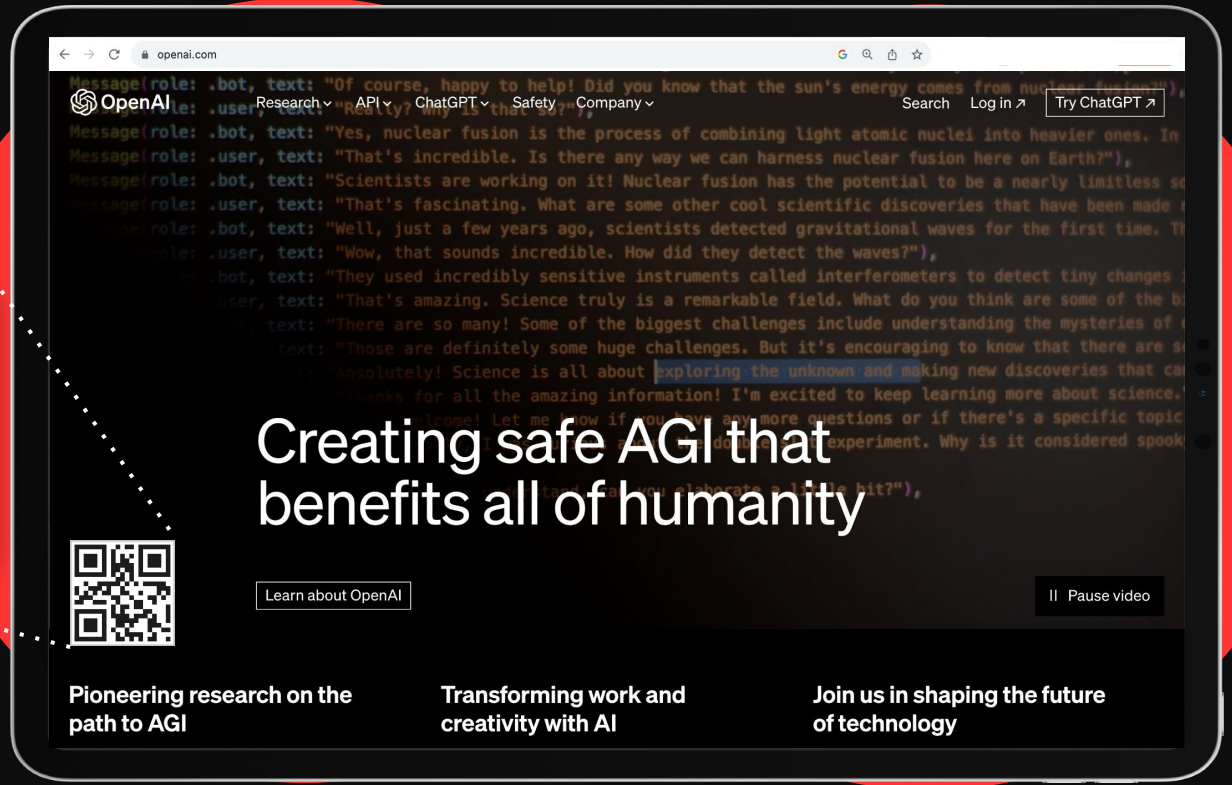
Vulnerabilidades

Reputación y valor en bolsa son una cortina de humo.
¿Nos debemos a...

- los usuarios?
- aquel que paga nuestro salario?

Industria: Cyber Labeling

"https://openai.com/well-known/sbom"



Exhibicionismo obligatorio

1. SBOM (SPDX ISO5962, CycloneDX)
2. SBOM + VEX
3. OpenSSF
4. CRA (UE DRAFT)
5. Cyber Labeling (SG, FI, DE)
6. SLSA
7. S2C2F

Dogfooding

01 Código fuente totalmente público:
https://gitlab.com/fluidattacks/universe/

02 Incidentes totalmente públicos:
https://status.fluidattacks.com/history

03 Disponibilidad y rendimiento totalmente públicos:
https://availability.fluidattacks.com/

04 OpenSSF nivel Gold:
https://www.bestpractices.dev/en/projects/6313

¡CISOs a la cárcel!

Abogado, fiscal en el DoJ, CISO de Ebay, Paypal, Airbnb, Facebook, Uber y Cloudflare, y asesor de Obama:

- Brecha y divulgación a FTC (2014)
- Brecha a 57M de usuarios (2016)
  - Oculta como un "bounty" de 100K USD
- Nuevo CEO **exhibe** lo sucedido (2017)
  - Dosis de **masoquismo** 148M (2018)
- 3Y de libertad condicional, 50K USD y 200h
  - "If I have a similar case tomorrow, even if the defendant had the character of Pope Francis, they would be going to prison," Judge Orrick

We hack
your software

www.fluidattacks.com