Telefónica Tech

ElevenLabs
ElevenPaths Innovation & Labs

C4IN
Cybersecurity 4 Industry

En busca de “El Dorado”

Ciberseguridad industrial

Telefónica Tech

#whoami

Sergio Vidal

Ingeniería informática

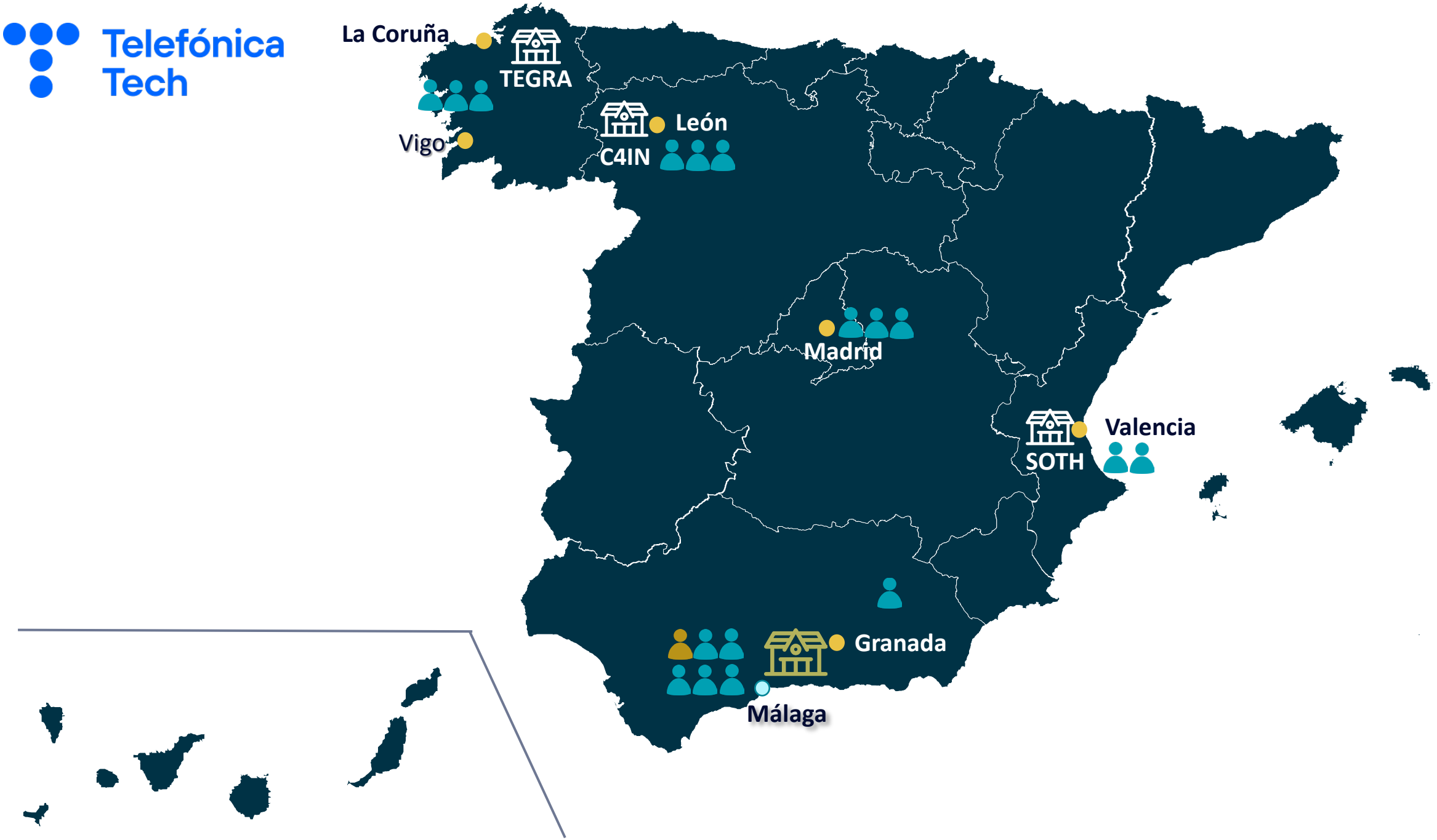
Máster en investigación en ciberseguridad

Universidad de León – IoT cybersecurity research

INCIBE-CERT – IR & Proactive services

Telefónica Tech – Innovación & Labs – OT cybersecurity research @ C4IN

Telefónica Tech



Telefónica Tech

- **6 herramientas o productos desarrollados y publicados**
- **4 tecnologías y propuestas innovadoras**

40 conferencias científicas y técnicas
15 cursos y workshops docentes

3 publicaciones de artículos o revistas científicas
5 artículos e informes técnicos

100 entradas de blog para divulgación
200 entradas cortas en RRSS
1 libro publicado anualmente

25 proyectos universitarios TFG o y TFM

25 acciones de asesoramiento técnico y científico
15% Patentes Telefónica

black hat DEFCON

EKOPARTY

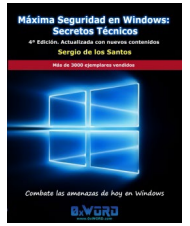
GUARDS FOR DIGITAL LIVES
SECURITY INNOVATION DAY

RSA CONFERENCE

Eleven Paths
CyberSecurityReport

WHITEPAPER
Nuevo informe sobre vulnerabilidades encontradas en Microsoft

Think Big / Empresas
CYBERSECURITY PULSE
Insights about security



Campus Internacional CIBERSEGURIDAD

TUTORÍA

talentum

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

incibe_

CYBER THREAT ALLIANCE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

ECS
EUROPEAN CYBER SECURITY ORGANISATION

EUROPOL

Google

Microsoft

MICROSOFT Digital Crimes Unit

Telefónica Tech

- **6 herramientas o productos desarrollados y publicados**
- **4 tecnologías y propuestas innovadoras**

40 conferencias científicas y técnicas
15 cursos y workshops docentes

3 publicaciones de artículos o revistas científicas
5 artículos e informes técnicos

100 entradas de blog para divulgación
200 entradas cortas en RRSS
1 libro publicado anualmente

25 proyectos universitarios TFG o y TFM

25 acciones de asesoramiento técnico y científico
15% Patentes Telefónica

Telefónica Tech

Ciberseguridad industrial

- ¿Quiénes somos?
- ¿De dónde venimos?
- ¿A dónde vamos?

¿Quiénes somos?

- IT vs OT
- Tecnología propietaria sólo auditable por el fabricante
- Difícil de simular – Difícil de validar
- Cada vez más dispositivos telemáticos
- Los dispositivos están desatendidos
- Menor atención a la seguridad
- La convergencia IT-OT expone a esta última
- Ataques específicos para el ámbito industrial
- Pérdida del “airgap”

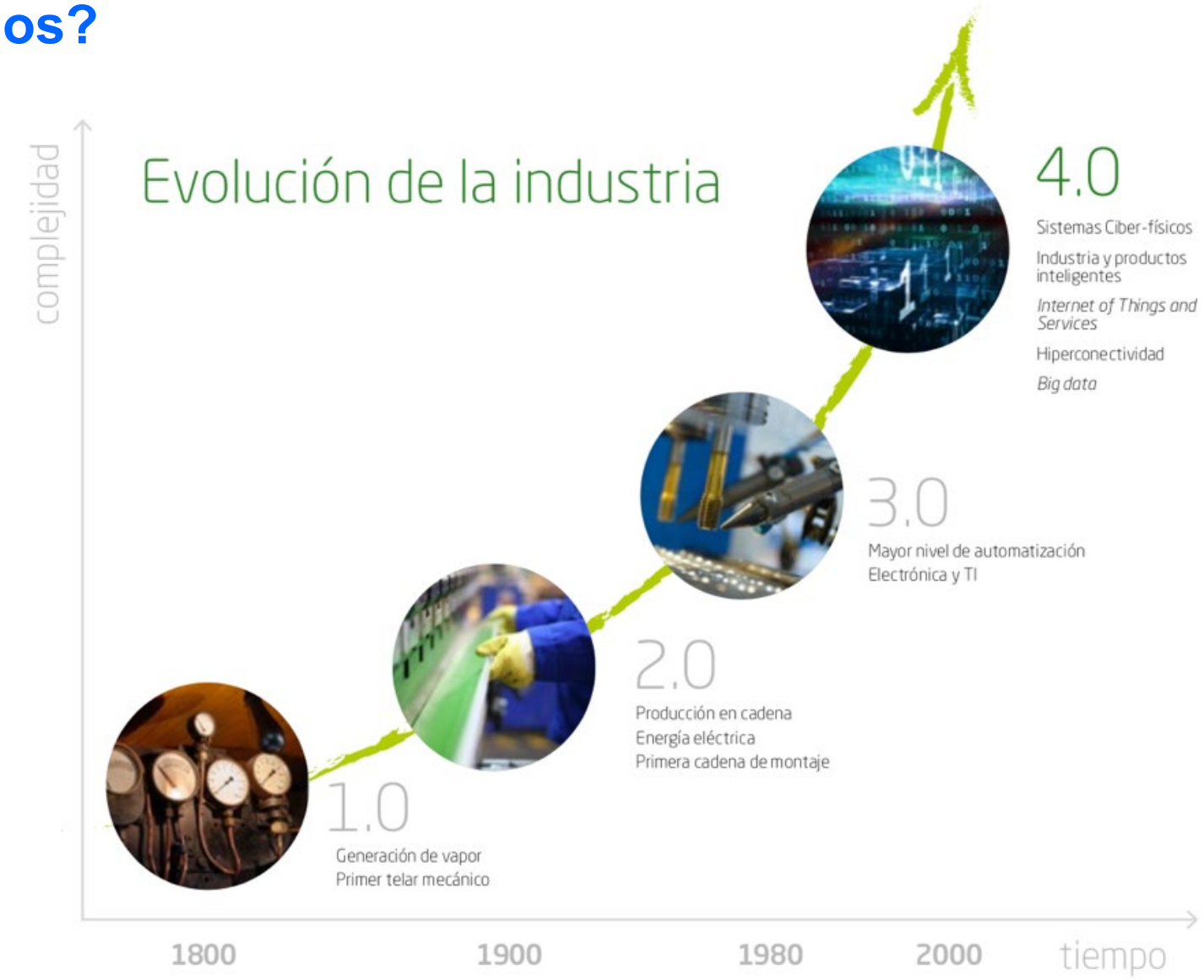
¿De dónde venimos?

- Los pilares de las tecnologías operacionales
- Durante muchas décadas, seguridad clásica
  - Rugerizado, inventariado, seguridad física…
- Industria de los 90s
  - DMZ, antivirus, controles de acceso
- Industria 4.0
  - SIEM
  - Threat Intelligence
  - Network monitoring

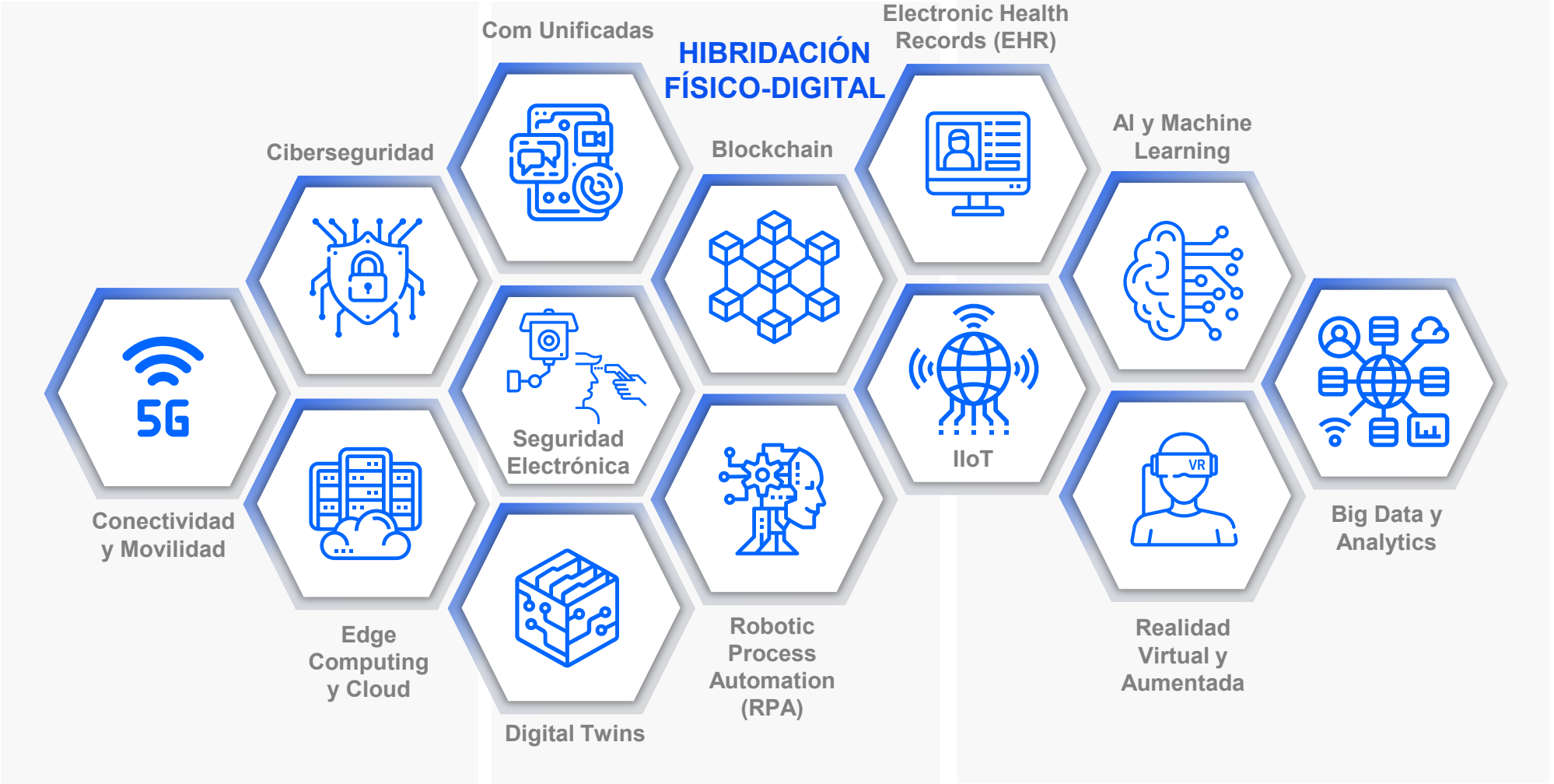
Concepto de superficie de ataque

Superficie de ataque real

¿A dónde vamos?

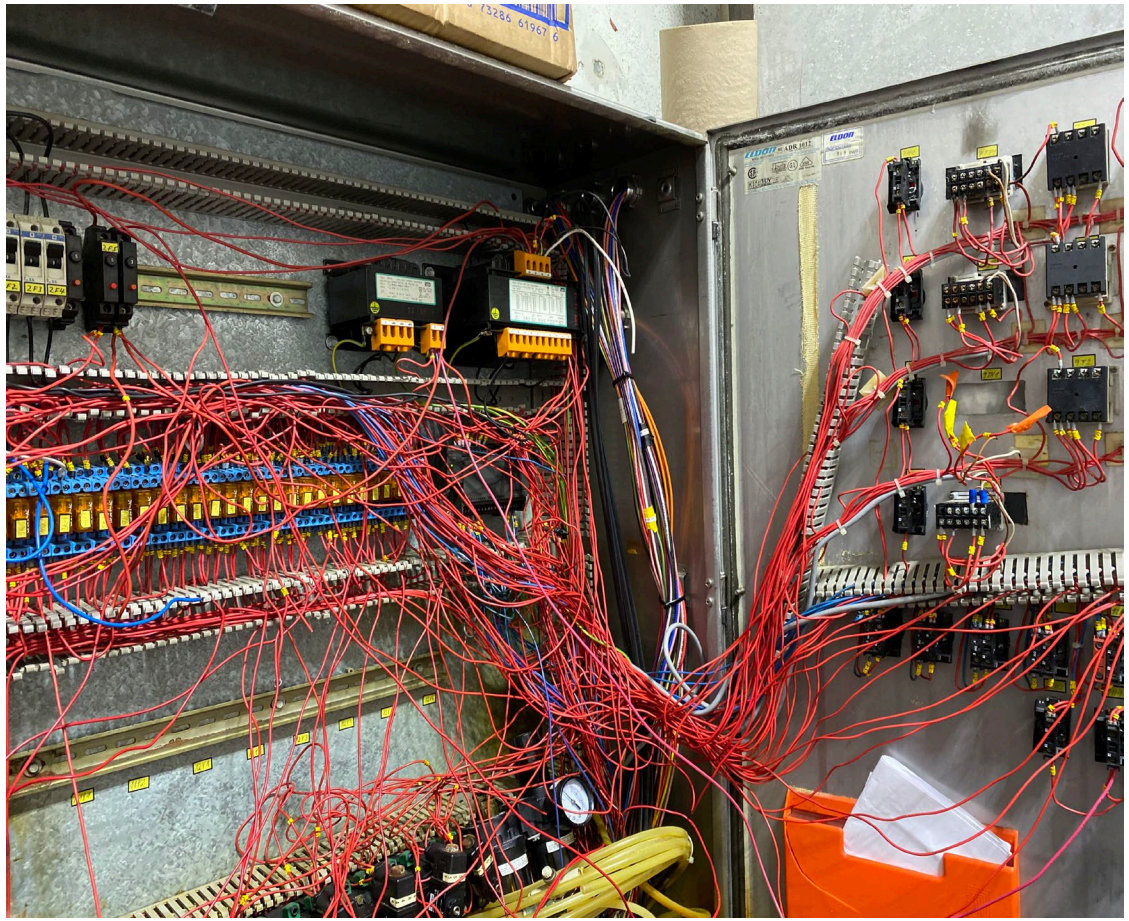


¿A dónde vamos?



Manos a la obra y … problemas

- **Construcción y adquisición de datos**
  - Honeypots
  - Virtualización
- **Selección de servicios a exponer**
- **Procesado y obtención de información útil**
- **Problemas y posibles soluciones**
- **Resultados**



LOS ENTORNOS INDUSTRIALES NO SON SIMULABLES

Telefónica Tech

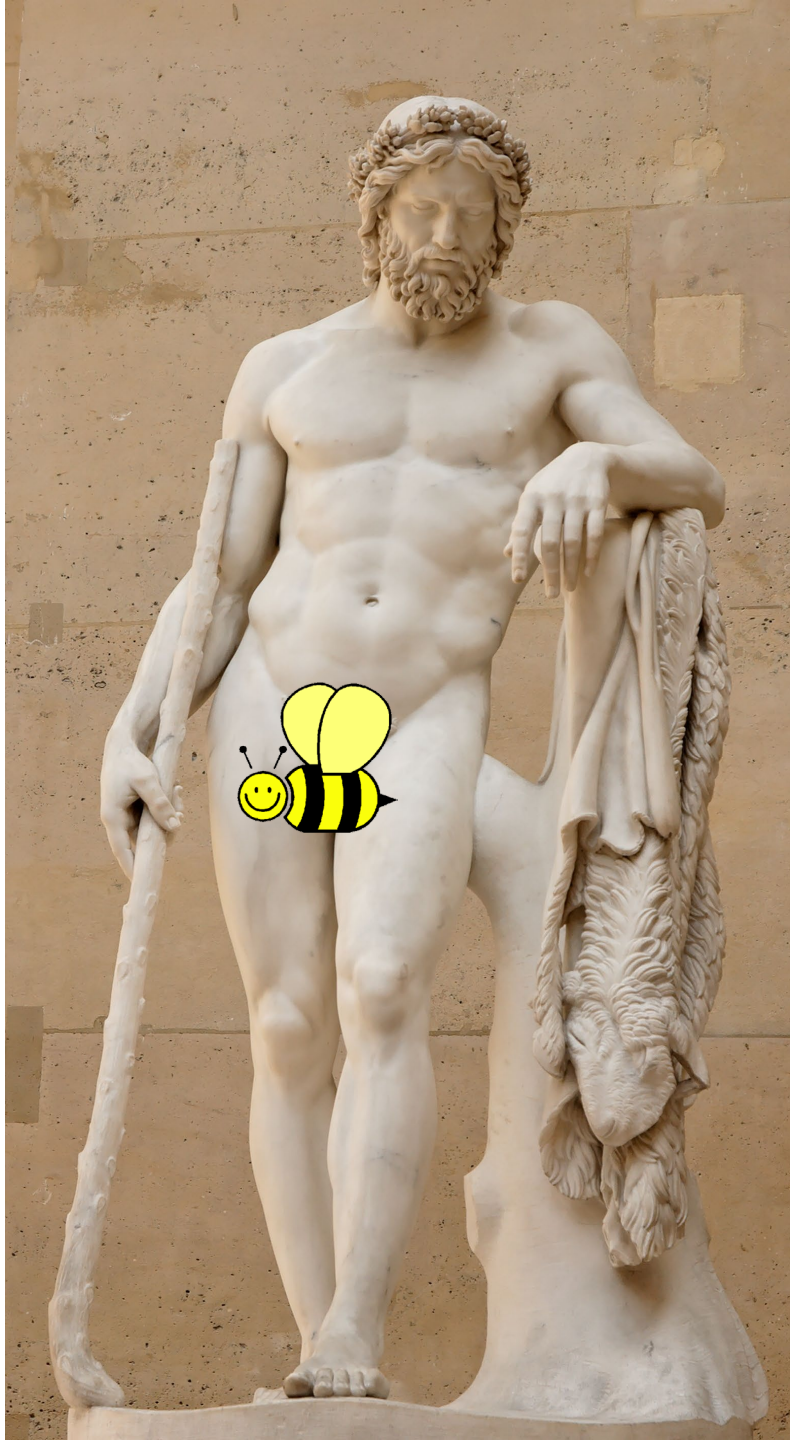
Aristeo – A **C4I**zó**N** quitado

Un poco de mitología

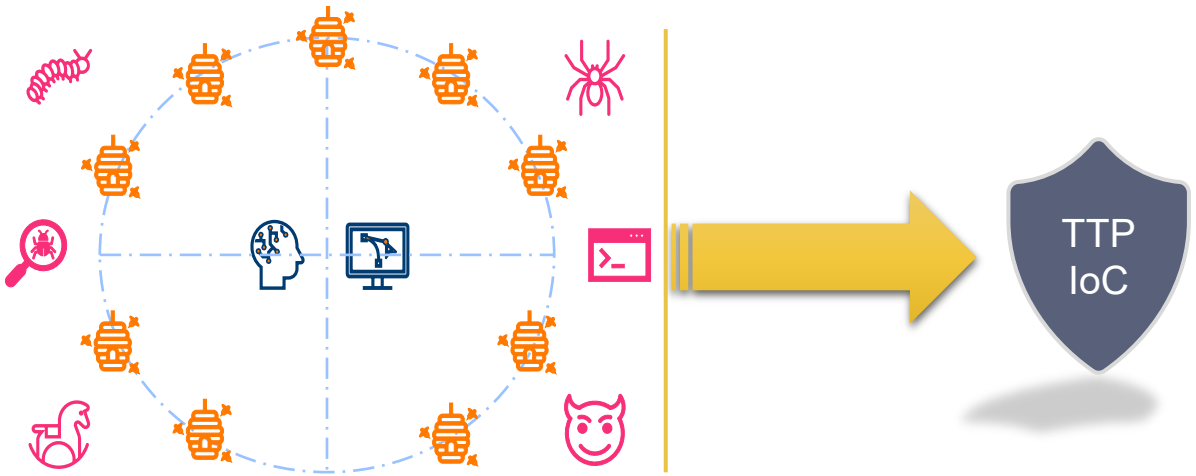
Aristeo (Aristaios: «el guardián de las abejas»). Dios menor de la mitología griega.

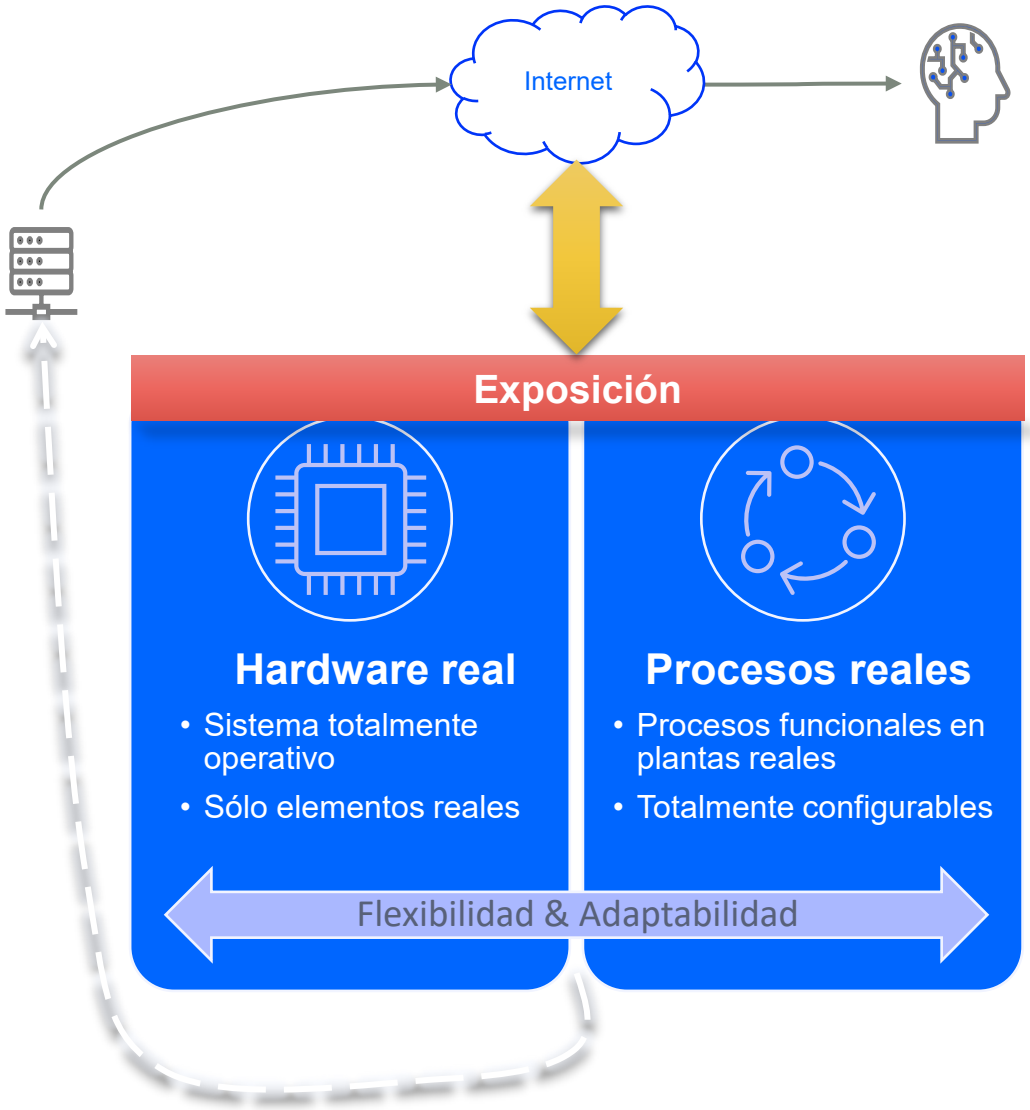
- Las Ninfas de mirto le enseñaron artes útiles y misterios. Entre otros, cómo domesticar las abejas y mantenerlas en las colmenas.

- Así se convirtió en el dios patrón del ganado, de los árboles frutales, de la caza, la agricultura y la apicultura.



Aristeo: Definición & Diseño





Definición: "Metahoneypot" industrial con hardware **real** para la extracción de inteligencia y análisis de amenazas propias de los ecosistemas OT.

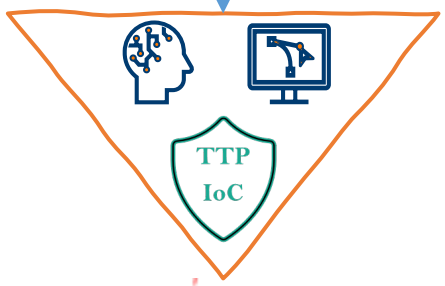
Meta: Establecer una red de honeypots industriales **reales** para el análisis de amenazas OT.

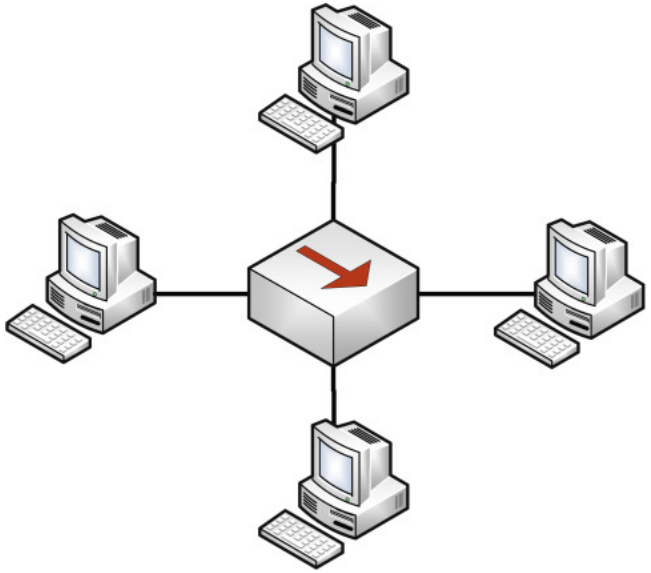
- Los entornos industriales son difíciles de simular virtualmente y la información obtenida pierde fidelidad. La información de entornos OT reales es escasa y no suele ser fiable, ya que se entremezclan entornos OT-IT y se tiende a virtualizar.

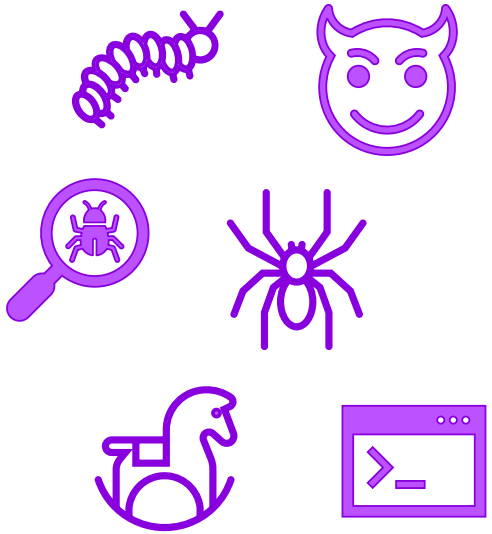
Características fundamentales: Flexibilidad y adaptabilidad

- Entornos adaptables a los diferentes tipos de procesos
- No ocupa el mismo espacio que las instalaciones reales

Telefónica Tech





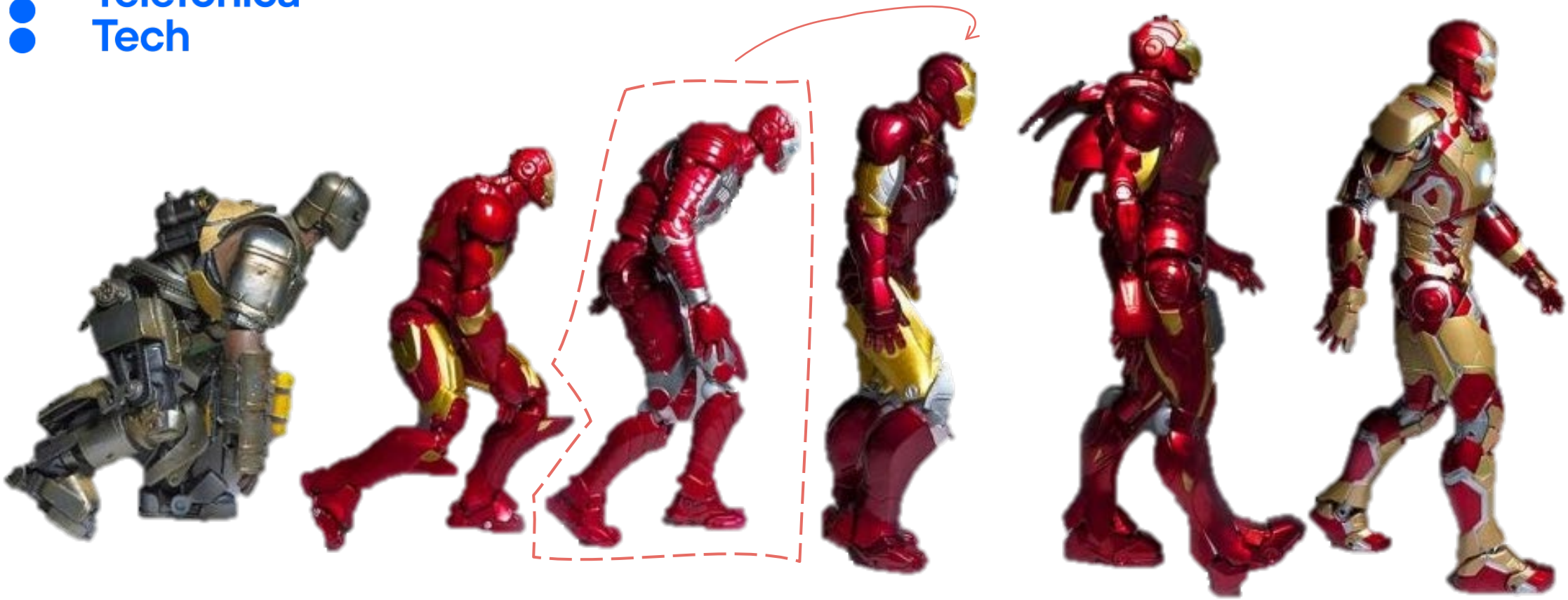


Funcionamiento y resultados

aristeo.elevenlabs.tech

Más de 650M de eventos registrados en 2021

Telefónica Tech



Honeypots y análisis IT

Entornos simulados

Entornos reales

Entornos reales con ML

Fusión de ámbitos IT-OT-IIoT-IoT

Gemelos digitales

La criptografía y los dispositivos industriales

- Los ecosistemas industriales contienen una gran variedad de dispositivos, muchos de estos con capacidades muy limitadas equiparables en potencia a muchos de los sistema embebidos

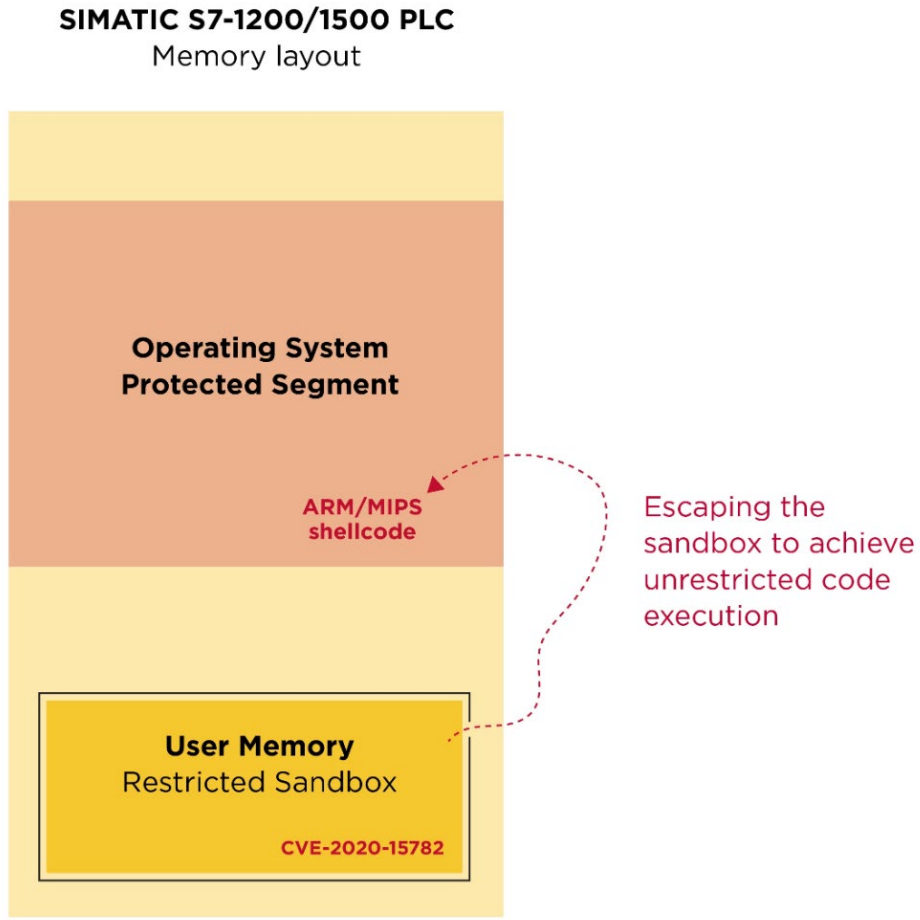
- Los dispositivos industriales tienen su lenguaje particular (texto estructurado, funciones de bloque, diagramas de escalera, …), en muchos de ellos no se pueden implementar de forma fácil operaciones como la rotación de bits

- Dispositivos como los PLC son usados principalmente para el control de los procesos, la ejecución de las operaciones en su tiempo exacto es muchas veces crítico. Con lo cual, la inclusión de operaciones computacionalmente complejas no es una tarea trivial

- La estructura y el acceso de la memoria de algunos dispositivos no es la ideal para almacenar “secretos” como pueden ser una clave privada

Casos recientes CVE-2022-38465

- CVSS v3 de 9.3
- Ejecución de código de forma remota para obtener las claves criptográficas globales hardcodeadas dentro de los PLC de la serie S7 desde un segmento de memoria con permiso de ejecución
- ¿Que puede hacer un atacante con estas claves?
  - Ataques avanzados contra el PC de control y los dispositivos asociados
  - Bypass de los 4 niveles de seguridad (no protection, write protection, write/read protection & complete protection)
  - Man-in-the-middle attacks
  - Cargas y descargas de código a los dispositivos
  - Interceptación y descifrado del tráfico de red




Telefónica Tech
Telefónica Cybersecurity & Cloud TECH
C4IN
Cybersecurity for Industry