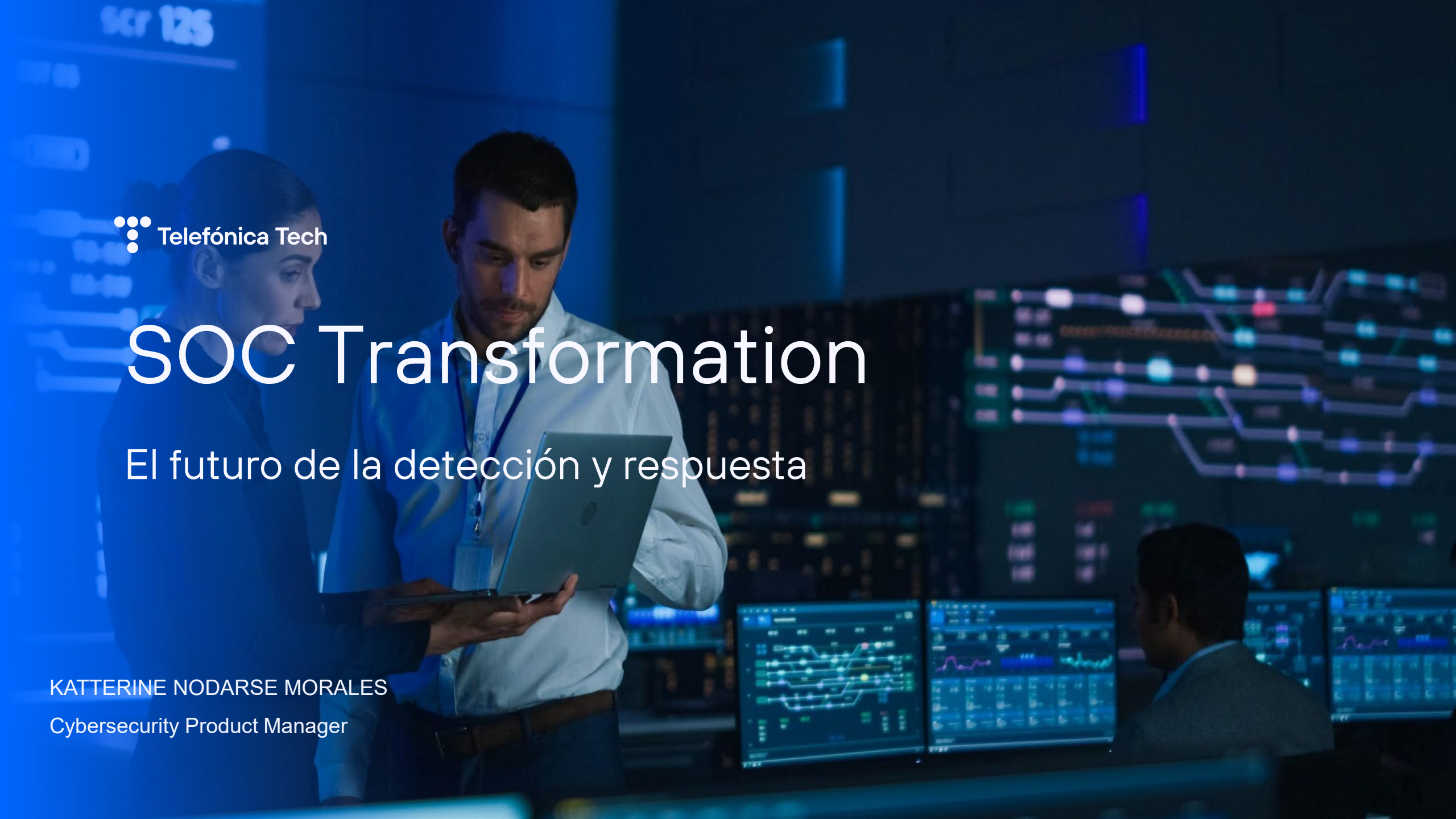


Telefónica Tech

# SOC Transformation

## El futuro de la detección y respuesta

KATTERINE NODARSE MORALES

Cybersecurity Product Manager

SOC DEL FUTURO

# Retos de la Detección y Respuesta en un nuevo contexto de ciberseguridad


Mayor superficie de ataque: Entornos híbridos, Cloud, trabajo en remoto, servicios de terceros, IA, etc.

Ataques mas rápidos y sofisticados: IA e hiper-automatización.

Situación geopolítica: ataques promocionados por estados,

Impacto global creciente de los ataques: económico, operativo y reputacional. Aumento del coste de perfiles especializados en ciberseguridad y formación continua.

Fragmentación de equipos y procesos: múltiples equipos con herramientas operadas en silos que no se comunican entre sí.

Atención de alertas individuales. No hay visión transversal de los incidentes.

Mantenimiento de sistemas y tecnologías.

Exposición de ataque desacoplada de la D&R

Falta de automatización/IA. los SOCs siguen dependiendo, principalmente, de procesos manuales

**MTTD/MTTR altos**

**Fatiga de alertas**

**Falsos positivos**

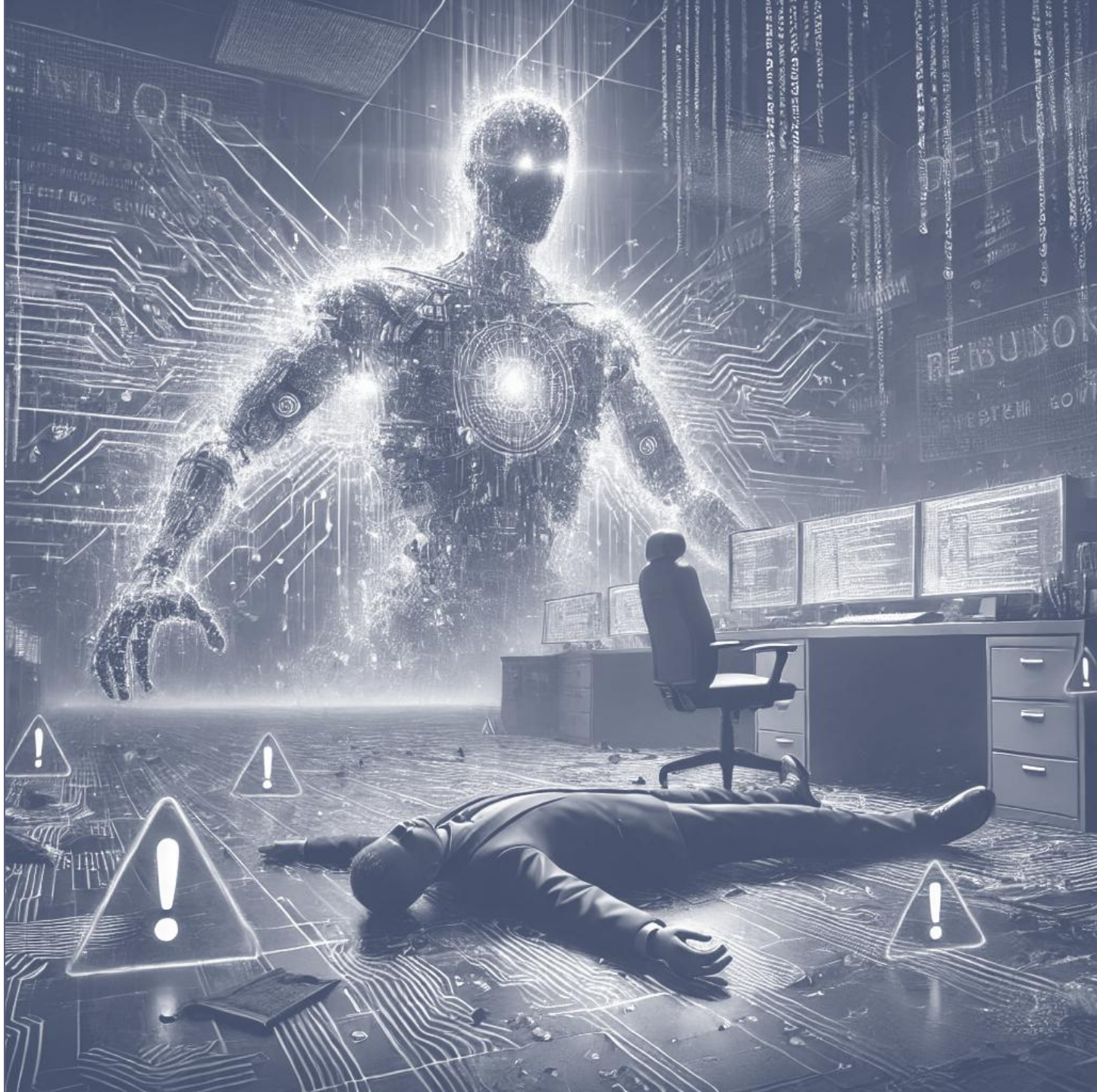
**Aumento del TCO**

**Puntos ciegos**

SOC DEL FUTURO

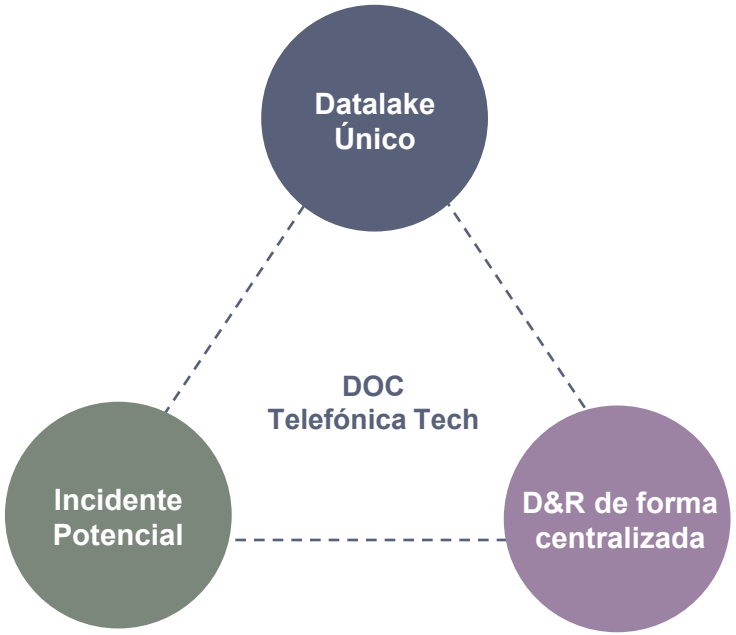
## El futuro con la automatización y la IA

# “El Analista vs *la máquina*”



Telefónica Tech | NextDefense

# Pilares para enfrentarse a estos desafíos



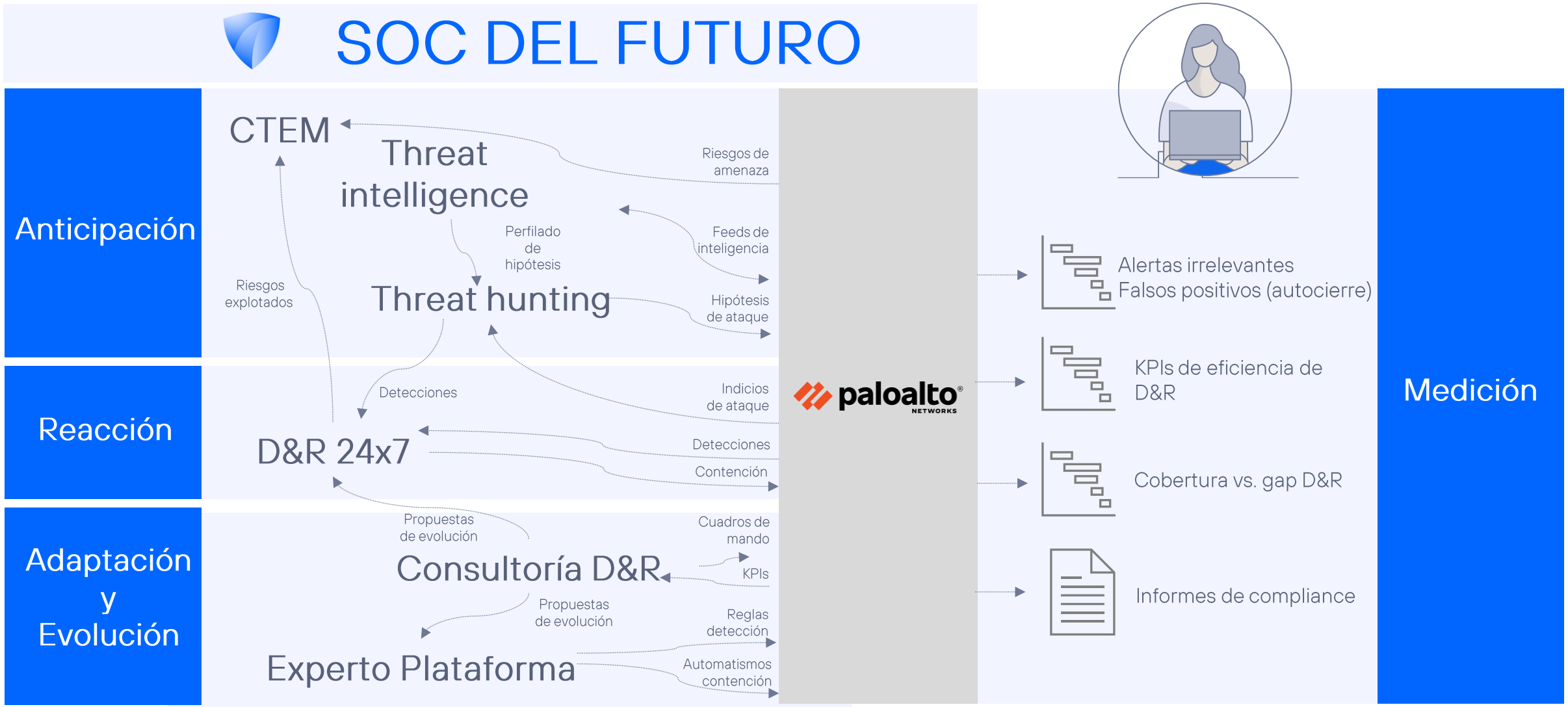

**Datalake único** con un modelo de datos único y un lenguaje de consulta también único. Se optimiza y facilita la detección.

**Incidente Potencial**: la agregación de un conjunto de señales o alertas susceptibles de causar un incidente real. Nos centramos en el incidente potencial, no en alertas aisladas.

**D&R Centralizada**: la idea no es ir a un modelo best-of-breed, si no a tener la capacidad de detectar y responder de forma centralizada: Menor carga operativa, detección y respuesta más eficiente, eficaz y rápida.

**La plataforma XSIAM es un facilitador/acelerador de la actividad de Detección y Respuesta de nuestro SOC. Va a permitir al SOC "elevar" su actividad para poder afrontar lo retos actuales apoyándose en la IA y la automatización.**

# SOC anticipativo, reactivo adaptativo y medible potenciado por una plataforma convergente



SOC DEL FUTURO

# Qué ofrecemos

## SERVICIO *CORE*

*POOL DE ANALISTAS D&R*

*INCIDENT MANAGER PARA INCIDENTES POTENCIALES*

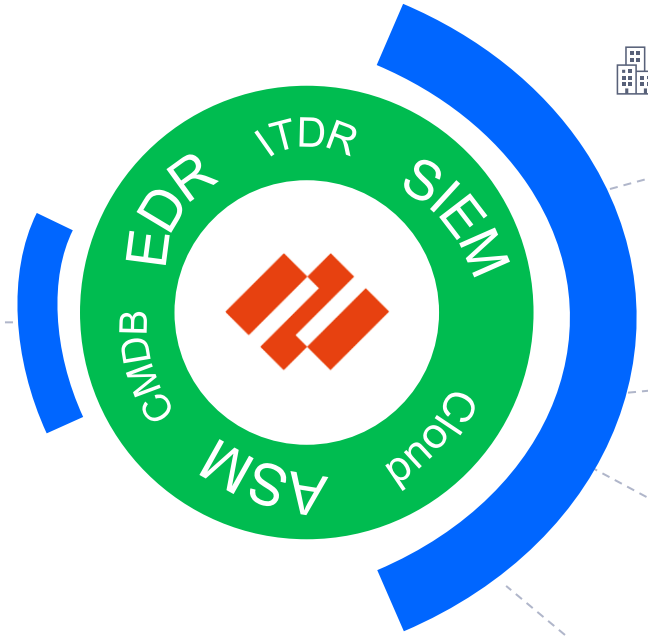
*CONSULTOR D&R PARA SEGUIMIENTO TRIMESTRAL*

*ALCANCE PREDEFINIDO DEL SERVICIO*

### DETECTION & RESPONSE 24x7

**EDR | SIEM** | IDENTITY | CLOUD

THREAT HUNTING aaS




## SERVICIOS DE VALOR AÑADIDO

*EVOLUCIÓN MEDIANTE PERSONALIZACIONES*

### THREAT HUNTING PERSONALIZADO

TI PROFILES | MANUAL HUNTS | AUTO HUNTS

### EXPERTO DE PLATAFORMA

REGLAS PERSONALIZADAS | PLAYBOOKS | PARSERS | PNR

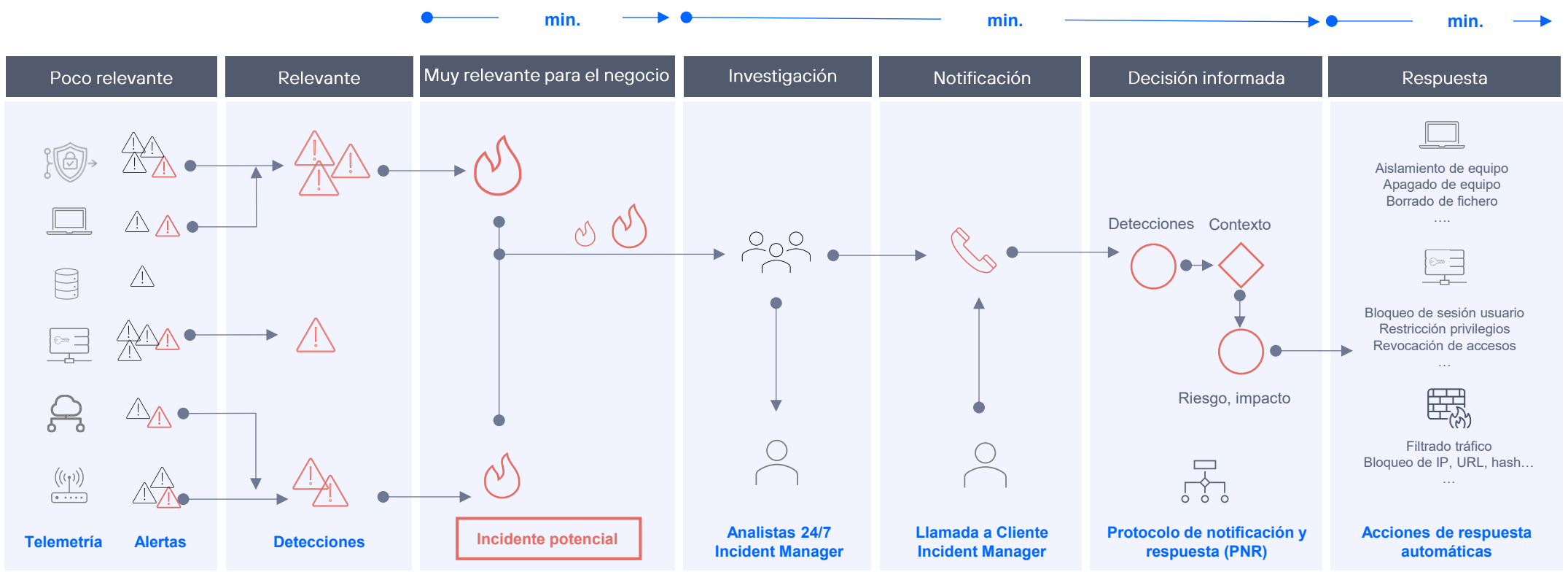
Recurso dedicado que no atiende alertas, porque su objetivo es evolucionar la plataforma acorde a las necesidades del Cliente.

### CONTINUOUS THREAT EXPOSURE MANAGEMENT

ASM | IDENTITY RISKS | CLOUD RISKS | VULNERABILITIES | TIP

SOC DEL FUTURO

# Operativa de D&R 24x7 holística, ágil y coherente con el contexto del negocio



SOC DEL FUTURO

# Detección y Respuesta 24x7: relevancia, priorización y evolución

### Una única cola operativa D&R 24x7

No fragmentamos la operativa por tecnología (SIEM, EDR, Identidad…)

### Respondemos de forma informada y coordinada

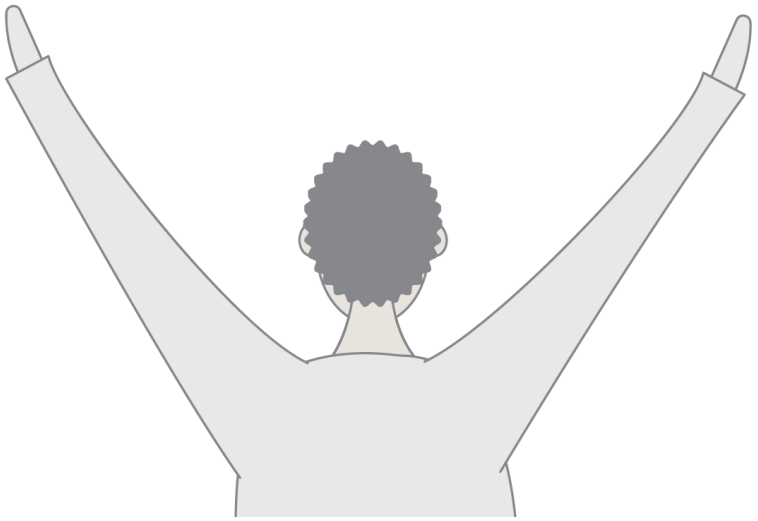
El PNR es la brújula específica para cada Cliente que nos guía sobre cómo enfocar la detección y la respuesta

### No atendemos alertas, sino incidentes con posible impacto en el negocio

Nuestro compromiso es el prevenir que un incidente comprometa el negocio, no atender el ruido de alertas irrelevantes

### Hacemos seguimiento de la eficiencia D&R

Hacemos una consultoría periódica basada en los datos y métricas para evaluar que reglas y automatismos de D&R funcionan y cuáles no



# ¿Por qué apostamos por Palo Alto en Telefónica?

1. Palo Alto es la compañía de seguridad IT más grande del mundo por capitalización de mercado. Pioneros en la estrategia de plataformización
2. Innovación continua + adquisiciones estratégicas que refuerzan su visión de plataforma.
3. Palo Alto y Telefónica Tech tienen el máximo nivel de partnership. Contamos con más de 300 personas certificadas en la tecnología
4. Contamos con certificaciones APS y ASC, posicionándonos como partner selecto y diferencial
5. NextDefense SOC es experto en tecnología de Palo Alto, servicios estándar + proyectos ad-hoc

## NextDefense SOC integra el 100% de la tecnología de Palo Alto Networks

Telefónica Portolio Conjunto

**GOVERN:** Advanced Security Management, Continuous Improvement & Compliance

**PREVENT:** CORTEX XPANSE · CORTEX CLOUD

**PROTECT:** STRATA · PRISMA SASE · PRISMA SD-WAN · PRISMA ACCESS

**RESPOND:** CORTEX XDR · CORTEX CLOUD · CORTEX XSIAM

CYBERARK

Cortex Extended Data Lake (XDL)

AGENTIX
XSIAM XSOAR

Capacidades Telefónica sobre Tecnologías Palo Alto

# ¿Quién es Telefónica Tech en Ciberseguridad?

Un proveedor global de **servicios de seguridad gestionada** con una cartera completa de capacidades de seguridad cibernética.

**15**
**AÑOS**
DE PRÁCTICA EN CIBERSEGURIDAD

**~2.000**
**CLIENTES**
DE CIBERSEGURIDAD A NIVEL GLOBAL

**MIEMBROS DE LA CYBER THREAT ALLIANCE**
EL ANTI-PHISHING WORKING GROUP Y LA RED NACIONAL DE SOC ESPAÑOLA

**>50**
**TECNOLOGÍAS**
Y MÁS DE 30 SERVICIOS DE CIBERSEGURIDAD GESTIONADOS

- **1.000** PLAYBOOKS DE AUTOMATIZACIÓN E INTELIGENCIA ARTIFICIAL DESPLEGADOS
- **>1M** ENDPOINTS PROTEGIDOS CON SERVICIOS DE DETECCIÓN Y RESPUESTA
- **>25K** DIRECCIONES IP ESCANEADAS CADA MES
- **>30K** APLICACIONES WEB ANALIZADAS MENSUALMENTE
- **>28K** HORAS DEDICADAS A SERVICIOS DE PENTESTING
- **100%** DE EJERCICIOS DEL RED TEAM EJECUTADOS CON ÉXITO
- **>20K** VULNERABILIDADES CRÍTICAS DETECTADAS AL MES EN ENTORNOS Y APLICACIONES CLOUD
- **>625K** ALERTAS DE SEGURIDAD GESTIONADAS
- **>2.000** INCIDENTES CRÍTICOS ATENDIDOS MENSUALMENTE EN ENTORNOS CLOUD
- **>20K** DISPOSITIVOS DE SEGURIDAD GESTIONADOS ACTIVAMENTE
- **>100K** CONEXIONES SDWAN SEGURAS DESPLEGADAS
- **>1,5M** USUARIOS PROTEGIDOS BAJO ARQUITECTURAS SASE
- **>100K** DISPOSITIVOS OT MONITORIZADOS

Telefónica Tech

Telefónica Tech