Telefónica Tech

¿Qué es el SOC del Futuro?

- Un centro de ciberseguridad **inteligente, automatizado y predictivo**.
- Integra datos de múltiples fuentes (redes, nube, endpoints, usuarios).
- Transforma la seguridad de **reactiva a proactiva**, con decisiones basadas en IA.

Objetivo principal: reducir tiempos de detección, respuesta y carga de trabajo.

Principales desafíos para los SOCs

- Infraestructuras híbridas difíciles de proteger
- Volumen de alertas (+333M eventos / 6 meses)
- Falta de visibilidad e interoperabilidad entre herramientas
- Presión regulatoria (GDPR, NIS2, CRA...)

"Más del 90% de los SOCs aún dependen de procesos manuales"

Transformación de las ciberamenazas

- Uso intensivo de IA por los atacantes.
- Aumento de vulnerabilidades explotadas (+55% en 2 años).
- Explosión de ataques con credenciales robadas (se ha multiplicado x5 en 2 años).
- Menor tiempo para actuar: de 9 días a menos de 2.

71%

ataques con credenciales robadas.

45%

de las exfiltraciones suceden en <1 día.

Evolución de la ciberseguridad integrada con la IA

- La Inteligencia Artificial y el Machine Learning priorizan amenazas, reducen alertas y mejoran la respuesta.
- Se ha conseguido la disminución de falsos positivos.
- Uso de LLMs para automatizar tareas repetitivas.

20–40% de las tareas de analistas pueden ser automatizadas

Detección en 10 segundos | Respuesta en 1 minuto

Del SOC tradicional al SOC del futuro

	SOC Tradicional	SOC con IA
Procesos	Manuales	Automatizados
Visibilidad	Parcial / en silos	Total y unificada
Alertas	Volumen excesivo	Filtrados inteligentes
Tiempo de reación	Lento	En tiempo real
Analistas	Saturados	Apoyados por IA

Arquitectura del SOC moderno