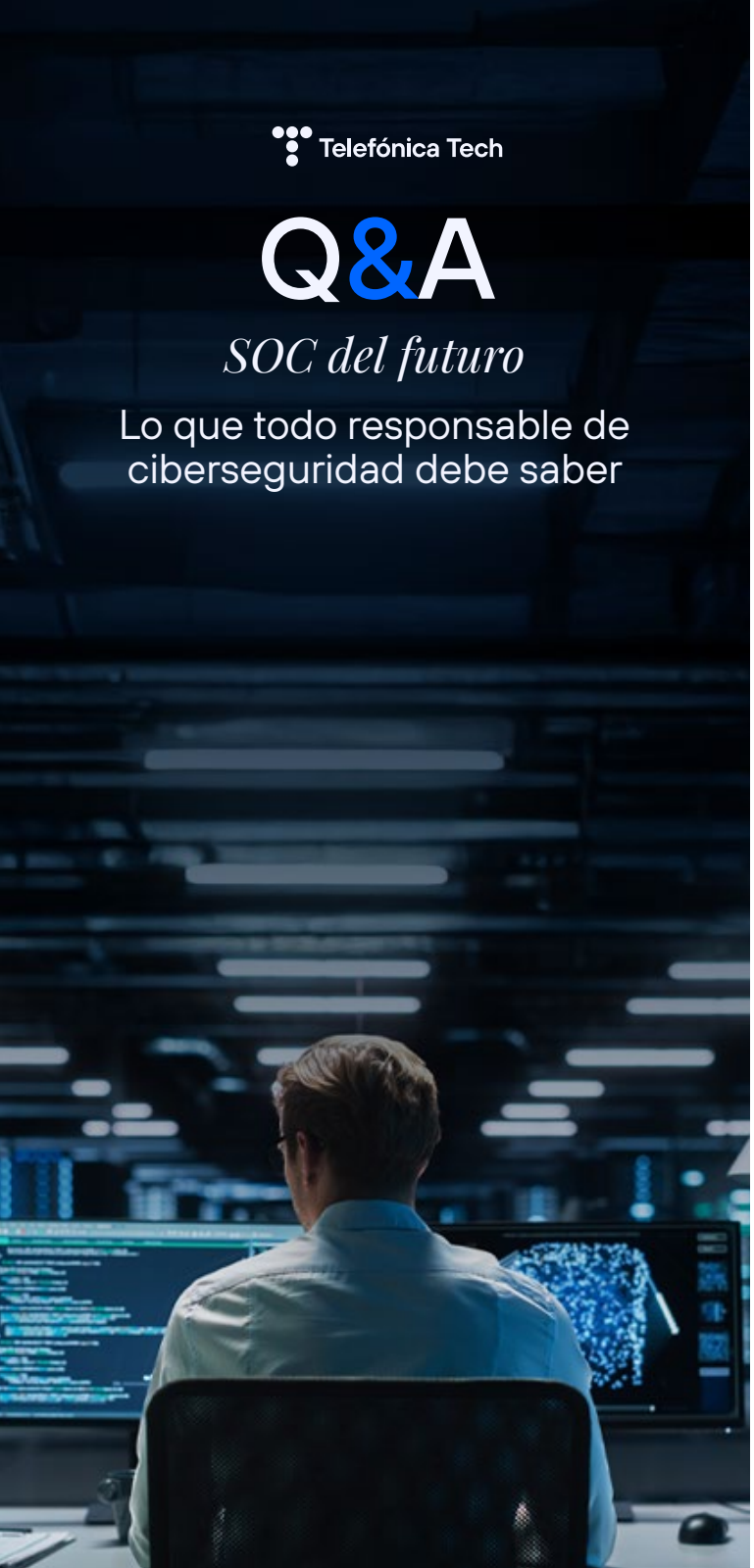

Telefónica Tech

Q&A

SOC del futuro

Lo que todo responsable de ciberseguridad debe saber

1. ¿CUÁLES SON LOS RETOS QUE AFRONTA UNA ORGANIZACIÓN CUANDO SU CENTRO DE OPERACIONES DE SEGURIDAD CUENTA CON MÚLTIPLES HERRAMIENTAS Y CARECE DE UN REPOSITORIO DE DATOS UNIFICADO?

- **Datos dispersos y desorganizados:** Gran volumen de datos de seguridad y aplicaciones almacenados en distintos lugares, sin un método estandarizado para su recolección y organización, lo que impide su uso efectivo en la detección y respuesta a amenazas.
- **Ineficiencia en la investigación de amenazas:** Los analistas pierden tiempo cambiando entre herramientas para recopilar información, lo que retrasa la respuesta a incidentes y reduce la eficiencia del equipo.
- **Aumento de la complejidad operativa:** La gestión de múltiples herramientas y la falta de una visión consolidada incrementan la complejidad del SOC, dificultando la identificación y gestión de riesgos.
- **Desafíos en el cumplimiento normativo:** La falta de centralización y trazabilidad dificulta cumplir con regulaciones como NIS2 o DORA, que exigen mayor control, visibilidad y capacidad de respuesta ante incidentes de seguridad.

2. ¿QUÉ INDICADORES DE MEJORA HAN EXPERIMENTADO LOS CLIENTES TRAS IMPLEMENTAR NUESTRA PROPUESTA DEL SOC DEL FUTURO?

↓ MTTR
de días a minutos.

Hasta un
100%
de tasa de cierre de incidentes relevante.

↓ 75%
en los incidentes que requieren investigación manual.

Visibilidad completa del entorno gracias a un
datalake unificado

3. ¿QUÉ HERRAMIENTAS DEBE TENER UN SOC PARA DETECTAR Y RESPONDER A LAS AMENAZAS ACTUALES DE FORMA RÁPIDA Y EFICIENTE?

Para detectar y responder eficazmente a las amenazas actuales, un SOC moderno debe contar con herramientas clave que aporten agilidad, visibilidad y automatización:

- **XDR (Detección y respuesta extendidas):** Amplía la visibilidad y correlación de amenazas en múltiples entornos (endpoint, red, nube).
- **SOAR (Orquestación, automatización y respuesta):** Estandariza y automatiza procesos, reduciendo la carga manual y acelerando la respuesta.
- **ASM (Gestión de la superficie de ataque):** Identifica y monitoriza activos expuestos para reducir puntos vulnerables antes de que sean atacados.
- **SIEM (Gestión de eventos e información de seguridad):** Centraliza, analiza y correlaciona datos de seguridad para detectar incidentes con mayor precisión.
- **Inteligencia artificial integrada:** Permite enfrentar amenazas complejas reduciendo drásticamente los tiempos de detección (MTTD) y respuesta (MTTR) y optimizando la eficiencia operativa del SOC. Entre el 20% y el 40% de las tareas de analistas de seguridad pueden ser automatizadas con IA generativa.

4. ¿CÓMO ASEGURA EL SOC DEL FUTURO DE TELEFÓNICA TECH UNA DETECCIÓN Y RESPUESTA EFICAZ, DIFERENCIAL Y EN MEJORA CONTINUA FRENTE A OTRAS SOLUCIONES DEL MERCADO?

El SOC del Futuro de Telefónica que integra la plataforma Cortex XSIAM de Palo Alto Networks, ofrece un enfoque diferencial centrado en la detección y respuesta contextualizada, automatizada y centralizada. En lugar de actuar sobre alertas aisladas, se priorizan los incidentes potenciales, lo que permite un análisis más inteligente y orientado a la toma de decisiones.

Además, Telefónica acompaña durante todo el ciclo de vida del servicio: desde la consultoría estratégica y técnica (SOC *Transformation*) hasta el despliegue, definición de casos de uso, automatización, operación 24/7 y mejora continua.

Este enfoque, basado en la adaptación constante al negocio y al entorno de amenazas, garantiza un modelo de seguridad sostenible, escalable y alineado con las necesidades reales del cliente.

El SOC del Futuro de Telefónica que integra la plataforma Cortex XSIAM de Palo Alto Networks, ofrece un enfoque diferencial centrado en la detección y respuesta contextualizada, automatizada y centralizada

5. ¿CÓMO PUEDO JUSTIFICAR ESTA INVERSIÓN EN MI ORGANIZACIÓN?

La propuesta del SOC del Futuro de Telefónica Tech está alineada con objetivos de negocio clave: reducción del riesgo, eficiencia operativa, cumplimiento normativo y resiliencia frente a amenazas avanzadas. No se trata solo de tecnología, sino de una evolución del modelo de seguridad hacia un enfoque más inteligente y orientado a la mejora continua.

Para más información **visita nuestro espacio de SOC del futuro**

Acerca de Telefónica Tech:

Telefónica Tech es un integrador de tecnología global, líder en transformación digital. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data o Inteligencia Artificial. En todas estas verticales, contamos tanto con nuestras propias tecnologías como también con los mejores ecosistemas de partners estratégicos y así nos lo reconocen tanto los analistas de la industria como nuestros clientes. Y todo ello es posible también gracias a nuestros hubs en España, UK, Alemania, Brasil e Hispam llegamos a más de 5,5 millones de clientes en más de 175 países.

Si tienes alguna duda y quieres saber más sobre cómo podemos ayudarte, por favor:

→ **CONTÁCTANOS**