Telefónica

AI-Native SecOps

La evolución de las operaciones de ciberseguridad en la era de la Inteligencia Artificial.

¿Cómo ha cambiado el paradigma?

La transformación afecta tanto al defensor como al atacante.

El negocio evoluciona:

- Los agentes de IA automatizan procesos y tareas.
- El software se desarrolla a velocidad de máquina.
- Los datos se convierten en el principal activo operativo.
- Las identidades ya no son únicamente humanas.
- Las decisiones comienzan a ser asistidas por IA.

El atacante evoluciona:

- Automatiza el reconocimiento y la explotación.
- Genera campañas de phishing altamente personalizadas.
- Reduce el tiempo entre vulnerabilidad y ataque.
- Escala operaciones con un coste mucho menor.
- Utiliza IA para adaptarse continuamente.

El SOC evolucionó. El reto también

SOC Tradicional — Augmented SOC — AI-Native SecOps

Cada etapa respondió a un reto diferente:

SOC	Augmented SOC	AI-Native SecOPS
Detectar y responder a incidentes.	Aumentar la capacidad del analista mediante automatización e inteligencia.	Operar en un entorno donde personas, agentes y plataformas colaboran de forma continua.

La siguiente evolución no consiste en añadir más herramientas.
Consiste en transformar el modelo operativo.

Del dato al conocimiento

El verdadero valor no está en generar más alertas. **Un AI-Native SecOps transforma millones de eventos en conocimiento accionable,** combinando datos, contexto e inteligencia para ayudar a personas y agentes a tomar mejores decisiones.

La ventaja competitiva ya no está en procesar más información, sino en **comprender mejor el contexto.**

AI-Native SecOps no consiste en añadir IA

No es una tecnología, es una nueva forma de operar.

NO ES

- Un chatbot conectado al SOC.
- Un copiloto para analistas.
- Un LLM integrado en una plataforma.
- Una automatización más.

SÍ ES

- Un modelo operativo diseñado para la IA.
- Contexto compartido entre personas y agentes.
- Decisiones basadas en conocimiento.
- Automatización gobernada.
- Evolución continua.

La IA deja de ser una capacidad adicional para convertirse en el núcleo de las operaciones.

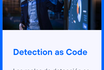
Security as Code

La seguridad evoluciona al mismo ritmo que el software.

Las capacidades de protección, detección y respuesta dejan de gestionarse manualmente.

Protection as Code

Las políticas de seguridad evolucionan de forma continua.



Detection as Code

Las reglas de detección se desarrollan, validan y versionan como software.

Response as Code

Las respuestas automatizadas se despliegan de forma consistente y repetible.

La seguridad deja de configurarse para empezar a **evolucionar continuamente.**

¿Qué caracteriza un AI-Native SecOps?

La IA amplifica el talento. No sustituye a las personas.

Las decisiones críticas siguen necesitando experiencia, criterio y conocimiento del negocio.
Las tareas repetitivas pueden automatizarse.

Inteligencia Artificial	Analistas
Analiza	Interpretan
Correlaciona	Priorizan
Automatiza	Deciden
Aprende	Supervisan
Escala	Gobiernan

El futuro no es Human vs AI. **Es Human + AI.**

Los principios de AI-Native SecOps

Cinco principios definen el nuevo modelo operativo.

Knowledge Driven
El conocimiento compartido impulsa cada decisión.

Security as Code
La seguridad evoluciona como el software.

Human + AI
Personas y agentes trabajan conjuntamente.

AI Governance
La IA opera bajo políticas, supervisión y control.

Continuous Evolution
Las operaciones mejoran continuamente a partir de la experiencia.

No es una plataforma. **Es un modelo operativo preparado para evolucionar.**

La visión de Telefónica Tech

Preparados para el siguiente paradigma.

En Telefónica Tech creemos que la evolución de las operaciones de ciberseguridad no pasa por incorporar más herramientas, sino por **construir un modelo operativo preparado** para un entorno donde la inteligencia artificial ya forma parte del negocio.

Nuestra visión combina **conocimiento, automatización, gobierno y colaboración entre personas y agentes** para ayudar a las organizaciones a operar con mayor resiliencia en la era de la IA.

El futuro de la ciberseguridad no consiste en añadir inteligencia artificial.
Consiste en construir operaciones capaces de trabajar con ella.