Telefónica

AI-Native SecOps

The evolution of cybersecurity operations in the age of Artificial Intelligence.

How has the paradigm changed?

The transformation affects both the defender and the attacker.

The business evolves

- AI agents automate processes and tasks.
- Software is developed at machine speed.
- Data becomes the primary operational asset.
- Identities are no longer exclusively human.
- Decisions are increasingly AI-assisted.

The attacker evolves

- Automates reconnaissance and exploitation.
- Generates highly personalised phishing campaigns.
- Reduces the time between vulnerability and attack.
- Scales operations at a much lower cost.
- Uses AI to continuously adapt.

The SOC has evolved. So has the challenge.

Traditional SOC — **Augmented SOC** — **AI-Native SecOps**

Each stage responded to a different challenge:

SOC	Augmented SOC	AI-Native SecOPS
Detect and respond to incidents.	Increase analyst capabilities through automation and intelligence.	Operate in an environment where people, agents and platforms collaborate continuously.

The next evolution is not about adding more tools.
It is about transforming the operating model.

From data to knowledge

The real value does not lie in generating more alerts. An AI-Native SecOps model **transforms millions of events into actionable knowledge**, combining data, context and intelligence to help people and agents make better decisions.

Competitive advantage is no longer about processing more information, but **about understanding context better.**

AI-Native SecOps is not about adding AI

It is not a technology. It is a new way of operating.

NOT

- A chatbot connected to the SOC.
- An analyst copilot.
- An LLM integrated into a platform.
- Another automation.

IT IS

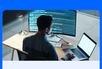
- An operating model designed for AI.
- Shared context between people and agents.
- Knowledge-driven decisions.
- Governed automation.
- Continuous evolution.

AI is no longer an additional capability. It becomes the core of operations.

Security as Code

Security evolves at the same pace as software.

Protection, detection and response capabilities are no longer managed manually.



Protection as Code

Security policies evolve continuously.

Detection as Code

Detection rules are developed, validated and versioned like software.

Response as Code

Automated responses are deployed consistently and repeatably.

Security moves from configuration to continuous evolution.

What characterises an AI-Native SecOps model?

AI amplifies talent. It does not replace people.

Critical decisions still require experience, judgement and knowledge of the business.
Repetitive tasks can be automated.

Inteligencia Artificial	Analistas
Analyses	Interpret
Correlates	Prioritise
Automates	Decide
Learns	Supervise
Scales	Govern

The future is not Human vs AI. **It is Human + AI.**

The principles of AI-Native SecOps

Five principles define the new operating model.

Knowledge Driven
El Shared knowledge drives every decision.

Security as Code
Security evolves like software.

Human + AI
People and agents work together.

AI Governance
AI operates under policies, oversight and control.

Continuous Evolution
Operations continuously improve through experience.

It is not a platform. **It is an operating model ready to evolve.**

Telefónica Tech's vision

Ready for the next paradigm.

At Telefónica Tech, we believe that the evolution of cybersecurity operations is not about adding more tools, but about **building an operating model designed for an environment where Artificial Intelligence** is already part of the business.

Our vision combines **knowledge, automation, governance and collaboration between people and agents** to help organisations operate with greater resilience in the age of AI.

The future of cybersecurity is not about adding Artificial Intelligence. **It is about building operations capable of working with it.**