Strengthening Cybersecurity with AI

Enhancing city security through advanced AI technologies

Capital Digital

MADRID

SMARTCITY
EXPO WORLD CONGRESS

Security with AI	Using artificial intelligence to enhance cybersecurity capabilities in protection and threat detection.
Security against AI	Defending against threats and attacks that leverage AI as an offensive tool.
Cybersecurity for AI	• Protecting artificial intelligence systems deployed within the organization from technical, ethical, and regulatory risks.
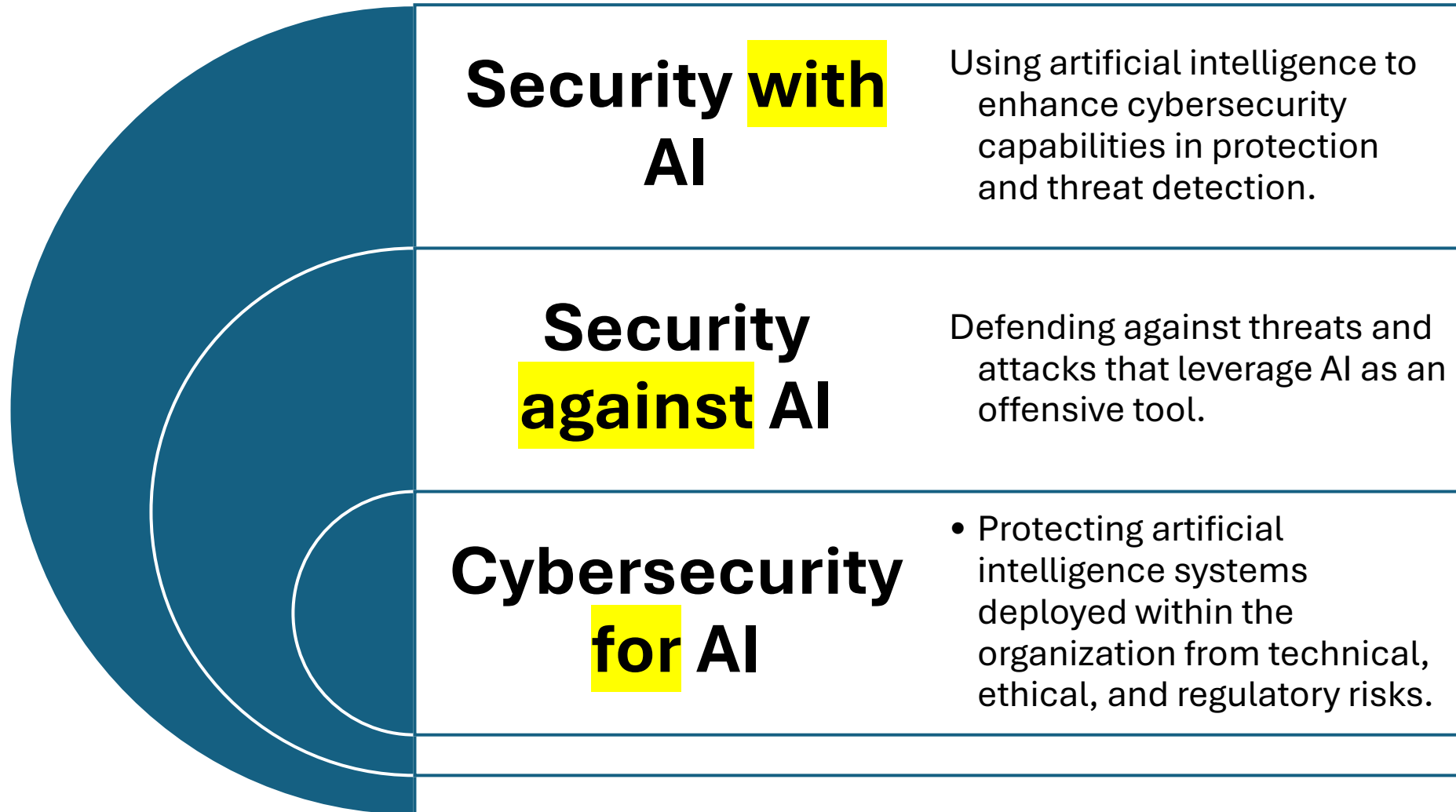
AI-powered threat detection and response

AI-assisted vulnerability management

AI-enhanced SOC operations (better response times, improving level 1 quality, optimized triage)

AI-based behavioral analysis

AI-driven automation of security tasks

Protection against AI-generated phishing and social engineering

Detection of deepfakes and synthetic media

Defense against adversarial AI attacks

Monitoring and mitigation of AI-driven malware

LAWFULNESS

Garantizando el cumplimiento de todas la leyes y reglamentos aplicables.

ETHICS

Respecting and guaranteeing adherence to ethical principles and values.

ROBUSTNESS

Both from a technical and social point of view, since AI systems, even if the intentions are good, can cause accidental damage.


Itinerario de Inteligencia Artificial
Marco Estratégico

Porque lo Digital es Capital
Madrid, Capital Digital

Chat AI

CMAD — Centro de Ciberseguridad Ayuntamiento de Madrid

TRANSPARENCIA

IMPACTO REAL

COORDINACIÓN

APLICABILIDAD

ÉTICA

CAPACITACIÓN

AI Conformance Assessment: The 5 Key Steps

Conduct conformity assessment where needed

5

Develop AI inventory

1

Check for transparency and sectoral obligations

4

Scan for prohibited practices

2

Assess risk levels across AI inventory

3

oxethica
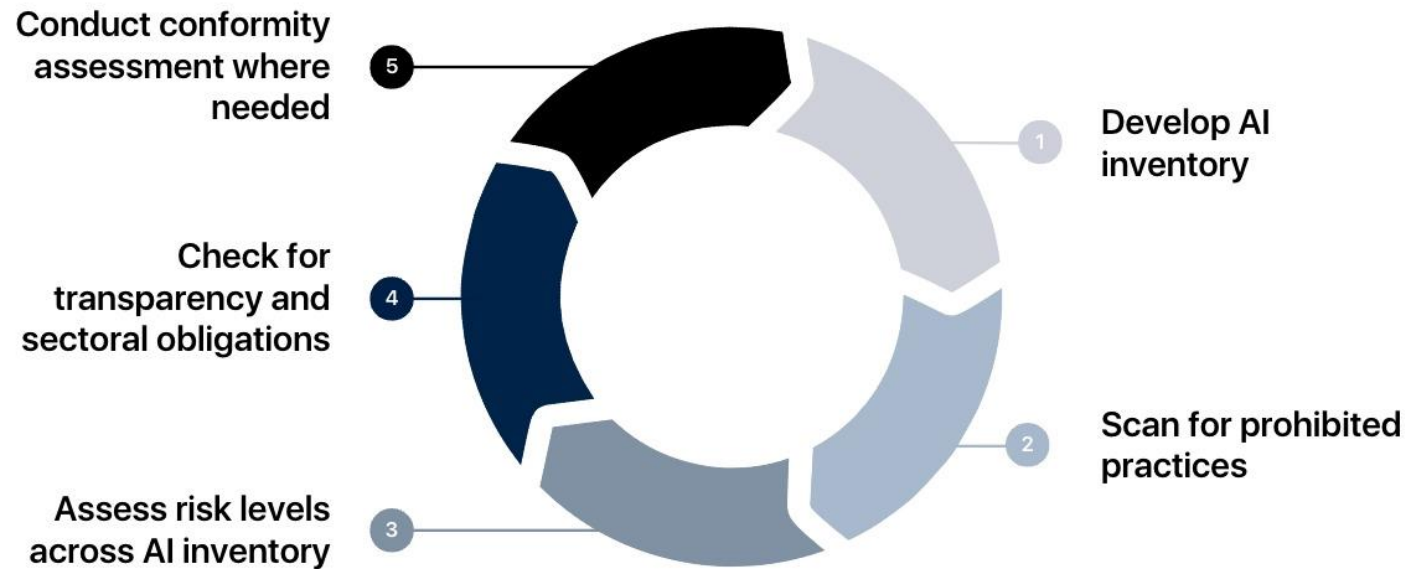
- 1ˢᵗ phase: Creation of an overview of all AI systems, current and planned:
  - What kind of AI system are we providing?
  - What databases and projects are connected to AI?
  - Is there any Personal Data processed?
  - Which is the level of risk?
- 2nd phase: Open Publication (AI inventory). Example: Helsinki