Esta presentación es para uso exclusivo para el evento de TIVIT Digital Innovation Day 2025 y debe tratarse con la debida confidencialidad.

No se debe compartir sin previa autorización de CyS Clientes y Estrategia SAS / C&S Customers and Strategy y Seccuri, Inc.

La IA *para* la seguridad y la IA *en contra* de la seguridad

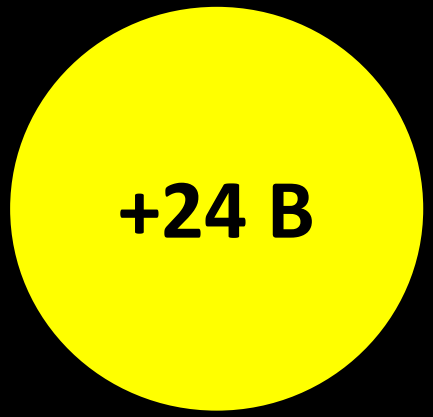
Juanita Duque

- Co-Fundadora y CEO de Seccuri
- VP Portafolio Ciber en CyS

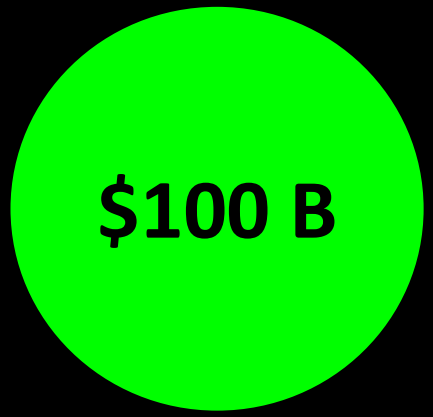
WEF reporte global de riesgos 2025

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

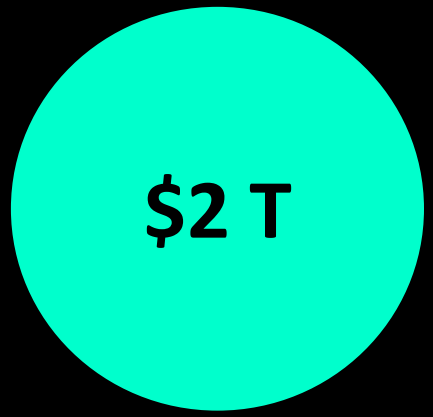
	2 años	10 años
1st	Misinformation and disinformation	Extreme weather events
2nd	Extreme weather events	Critical change to Earth systems
3rd	State based armed conflict	Biodiversity loss and ecosystem collapse
4th	Societal polarization	Natural resource shortages
5th	Cyber espionage and warfare	Misinformation and disinformation
6th	Pollution	Adverse outcomes of AI technologies
7th	Inequality	Inequality
8th	Involuntary migration	Societal polarization
9th	Geoeconomic confrontation	Cyber espionage and warfare
10th	Erosion of human rights	Pollution



Mercado para IA para ciberseguridad



Crecimiento para el 2030



Oportunidad para proveedores de ciberseguridad

Doble rol de IA

- La IA no es neutral
- Amplifica la protección, defensa y las amenazas
- Naturaleza de doble uso: mismos algoritmos, distintas aplicaciones
- Pregunta para hacernos: ¿Cómo podemos mantener el control cuando ambos bandos usan IA?

Inversión ciberseguridad basada en IA

94%

Empresas **ya usan IA** en su stack de ciberseguridad

62%

Pueden **predecir** ataques futuros

+60%

Defensas

Ataques

93%

Profesionales **saben** de ataques basados en IA

77%

Empresas han **sufrido** de ataques con IA

+$24T

Ciber crimen para 2027

IA Defensiva

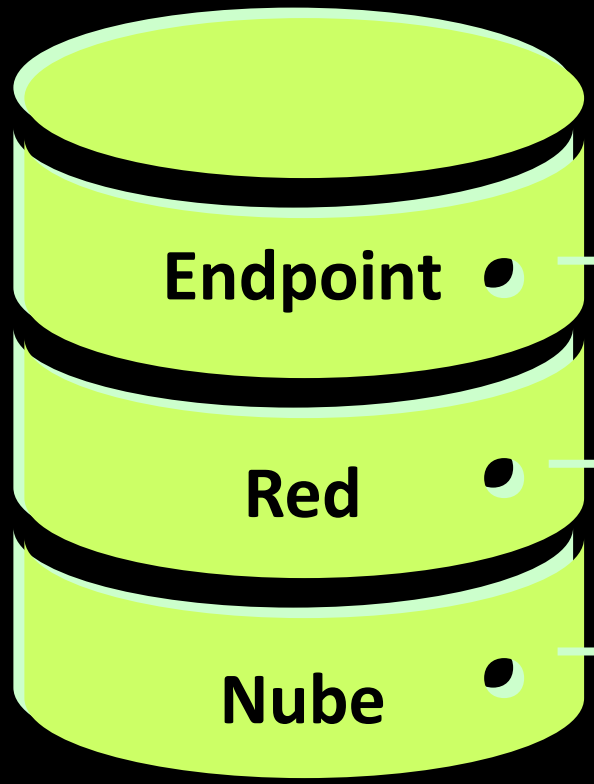
Inteligencia de amenazas
(NLP para extraer IOCs)

Detección de anomalías
(autoencoders, clustering)

Respuesta automatizada
(SOAR con aprendizaje automático)

Analítica predictiva
(modelos de series temporales)

Arquitectura Defensiva



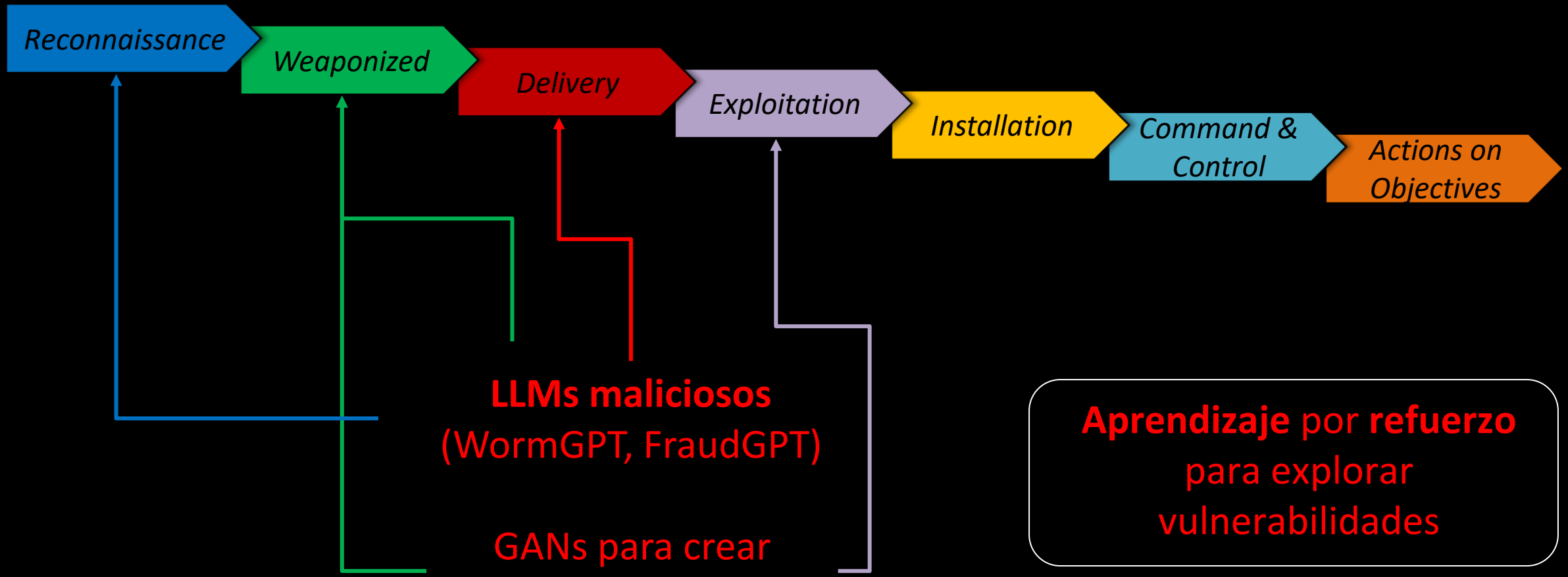
Protección de endpoints: aprendizaje federado

Seguridad de red: inspección profunda con redes neuronales

Seguridad en la nube: detección de anomalías en IAM

IA en la pila de seguridad

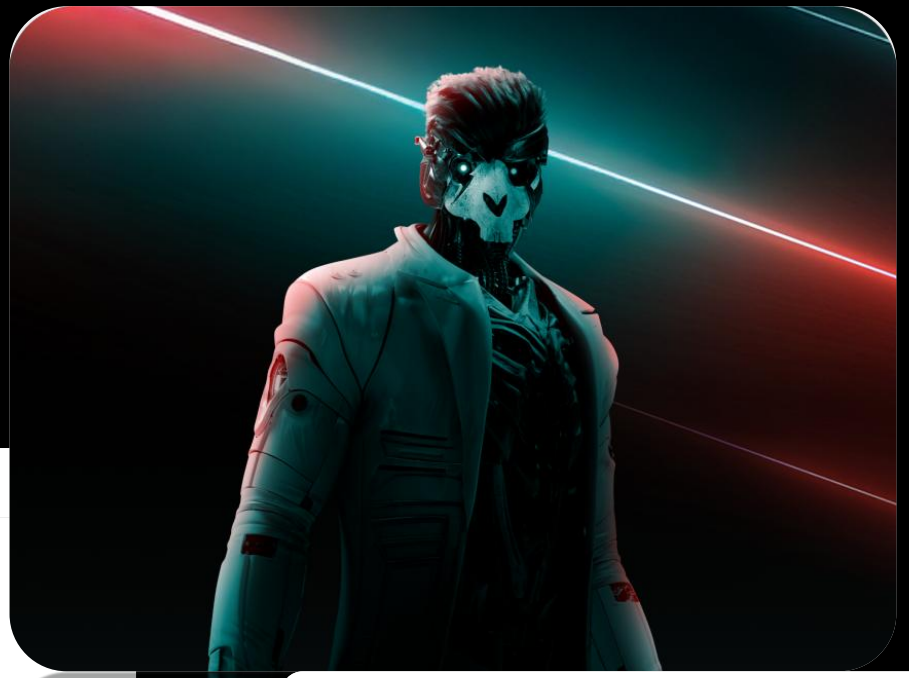
IA Ofensiva



Aprendizaje por **refuerzo** para explorar vulnerabilidades

Ejemplos de IA maliciosa

Generación de medios sintéticos



WORLD ECONOMIC FORUM

Join us

EMERGING TECHNOLOGIES

‘This happens more frequently than people realize’: Arup chief on the lessons learned from a $25m deepfake crime

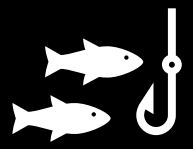
Feb 4, 2025

Famous Chollima

North Korea

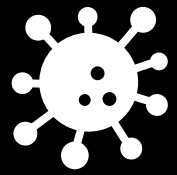
Ejemplos de IA maliciosa

Phishing



- Robo de credenciales
- Redacción automática con NLP

Malware



- Código polimórfico
- Evolución con modelos generativos

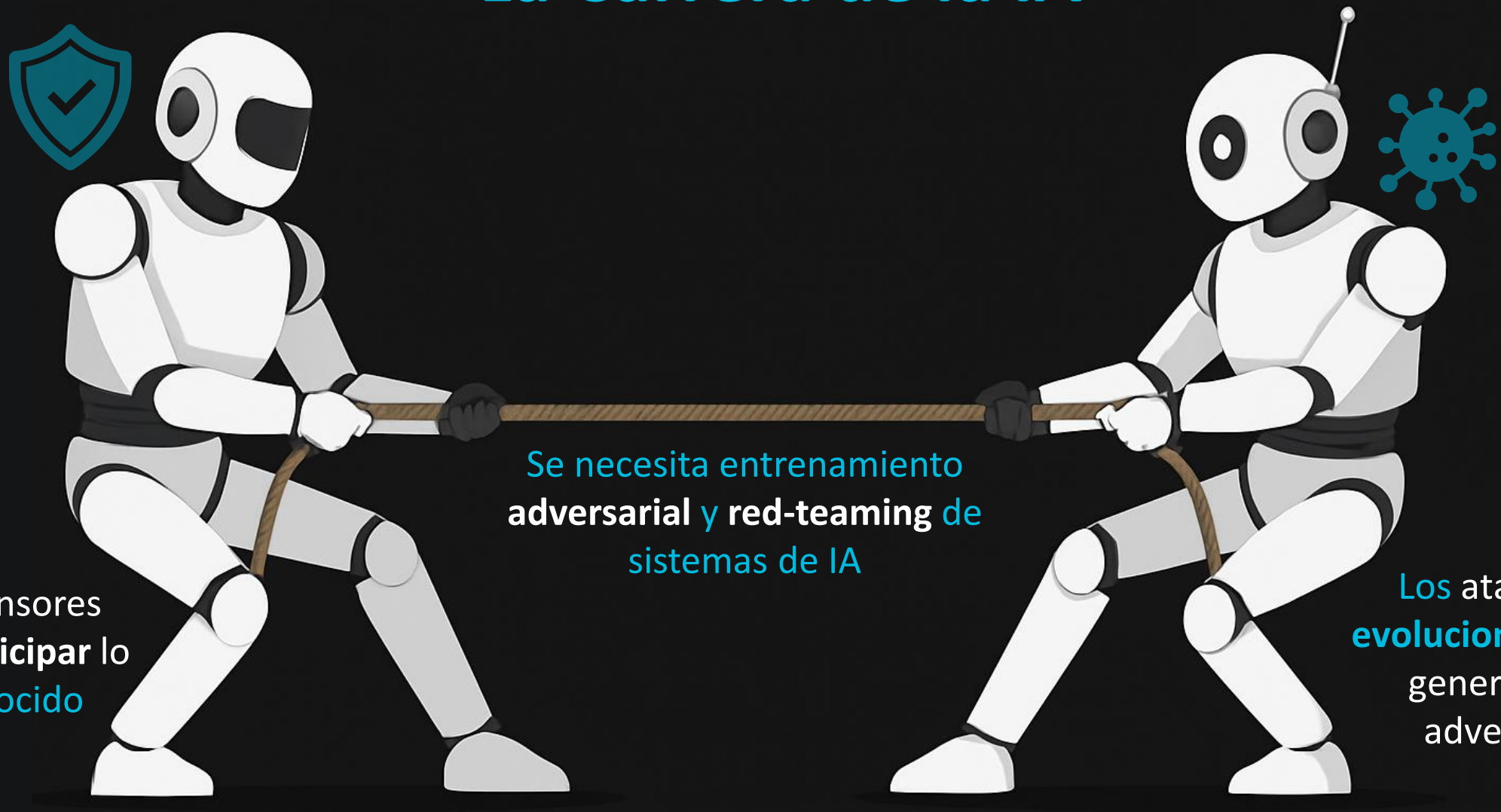
Ejemplos de IA maliciosa

- *Jockeroo*
- *Locky*
- *Goliath*
- *Stampado*
- *Encryptor*
- *Shark*

Modelos de ingresos **RaaS**

1. Suscripción mensual
2. Programa de afiliación – suscripción + 20 - 30% ingresos
3. Costo de licencia
4. Distribución de ingresos

La Carrera de la IA



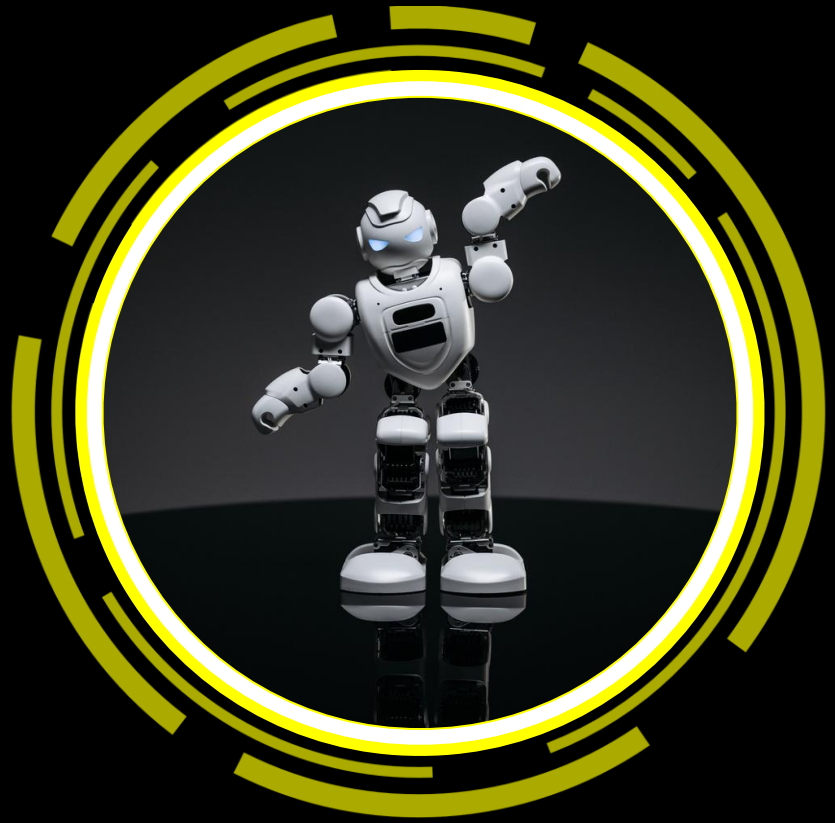
Los defensores deben **anticipar** lo desconocido

Se necesita entrenamiento **adversarial** y **red-teaming** de sistemas de IA

Los atacantes **evolucionan** con IA generativa y adversaria

¿Por qué no es fácil defender con IA?

- La IA defensiva requiere precisión, velocidad y confianza del analista.
  - Model Drift
    - Falsos positivos/negativos
      - Explicabilidad (SHAP, LIME)
        - Latencia

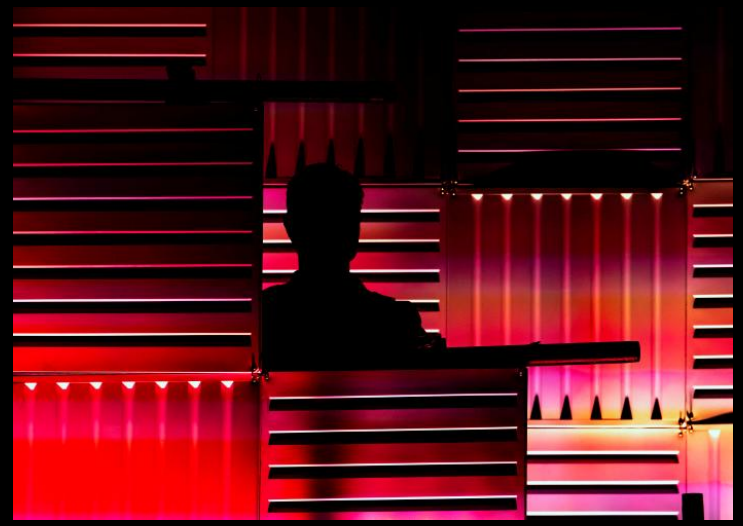


Agentic IA vs Talento de Ciberseguridad

- IA esta argumentando talento, no remplazándolo

- Hay bajas en roles de ciberseguridad:
  - Cybersecurity software engineer: ↓38%
  - IAM engineer: ↓26.5%
  - Security analyst: ↓13%

- Roles híbridos:
  - AI Security Analyst
  - Adversarial ML Specialist
  - Secure ML Pipeline Engineer



CSOnline, WSJ 2025

Estrategia de gobierno y mitigación

Pipelines de ML seguros

Sandboxing, fuente de información

Auditoría de modelos

Validación input adversario

Evaluación ética

Evaluación riesgo dual-use, líneas rojas

Estrategia para navegar el futuro de la IA en seguridad

- La IA amplifica capacidades, no intenciones
- La resiliencia adversarial es clave
- Se requiere colaboración entre IA, ciberseguridad y política

La IA no es buena ni mala → Es poderosa → Necesita dirección estratégica

IA está aquí para quedarse

IA es multiplicador de fuerza

- IA mejora la velocidad, precisión y escalabilidad defensiva y ofensiva
- Se necesita transparencia y gobernanza sólida

Revisión humana sigue siendo clave

- Integración estratégica requiere colaboración interdisciplinaria
- Marcos éticos deben guiar cada implementación

En que debemos enfocarnos

- Invertir en IA explicable y arquitecturas resilientes
- Priorizar integridad de los datos y la robustez
- Fomentar la cooperación global en estándares de seguridad

GRACIAS!


seccuri
Contáctanos!
contact@seccuri.com
https://www.seccuri.com