THREAT MODELING MULTI-AGENTE

AgenticTM

Threat modeling que escala

45~90
min
vs 3-5 días

$0
con Ollama local

12
agentes especializados

Open source, 2026

THREATX SECURITY

PhiloCyber

01
El problema

Threat modeling manual toma 3-5 días por sistema.

Con docenas de microservicios en pipeline, las cuentas no cierran.

THREATX SECURITY

PhiloCyber

02
Un analista, una perspectiva

- El especialista en cloud no ve amenazas de aplicación
- El experto en web no ve infraestructura
- Nadie está capacitado en amenazas AI/LLM

"Cinco ciegos tocan un elefante. Cada uno ve solo una parte."

THREATX SECURITY

PhiloCyber

EL CONCEPTO

La idea

¿Y si en lugar de un analista, tuviéramos 10 expertos trabajando juntos?

Una perspectiva

Análisis limitado, enfoque único.

Diez perspectivas

Inteligencia colectiva, cobertura integral.

AgenticTM: Multiplicando la capacidad de análisis

THREATX SECURITY

PhiloCyber

AgenticTM

Un equipo virtual de 11 agentes especializados.

ENFOQUE TRADICIONAL
(Manual)

3-5 DÍAS

Tiempo promedio por sistema

COSTO X

Consultores externos

2 METODOLOGÍAS

Análisis secuencial limitado

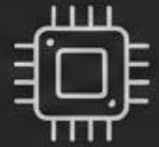
ENFOQUE AGENTICTM
(Automatizado)

45-90 MINUTOS

Tiempo total de ejecución

$0 COSTO

Ollama local (Privacidad total, sin fees)



5 METODOLOGÍAS

Ejecución paralela simultánea

Nota: Los tiempos pueden variar según la complejidad del sistema y el hardware local utilizado.

THREATX SECURITY

PhiloCyber

INSPIRACIÓN INESPERADA

TradingAgents: un sistema de trading multi-agente de Wall Street.
Adaptamos su arquitectura a ciberseguridad.

TradingAgents

- 5 analistas financieros
- Bull vs Bear
- Research Manager
- Decisión de trading

AgenticTM

- 5 analistas de seguridad
- Red Team vs Blue Team
- Threat Synthesizer
- Threat model profesional

THREATX SECURITY

PhiloCyber

07 El pipeline

MULTI-METHODOLOGY APPROACH

5 metodologías en paralelo

01

STRIDE

Microsoft, 1999
(Inter)

6 categorías: Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation

02

PASTA

VerSprite, 2012

7 etapas de análisis de riesgo orientado al negocio

03

Attack Trees

Schneier, 1999

Árboles jerárquicos AND/OR con cheapest path

04

MAESTRO

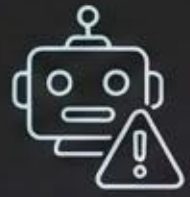
CSA, 2024

7 capas de seguridad para sistemas AI

05

AI Threat

OWASP, 2025



OWASP LLM Top 10 + Agentic AI + Protocolos

Cada metodología atrapa lo que las otras pasan por alto.

THREATX SECURITY

PhiloCyber

09 DEBATE ADVERSARIAL

THREAT MODELING PROCESS

RED TEAM

Escala amenazas

- Encuentra nuevos vectores
- Propone cadenas de ataque
- Desafía suposiciones

BLUE TEAM

Defiende con controles

- Contra-argumenta
- Propone mitigaciones
- Referencias NIST/OWASP

SEÑALES DE RESPUESTA

[CONCEDE] [DISPUTE] [MODERATE] [CONVERGENCIA]

THREATX SECURITY

PhiloCyber

Sistema RAG

Memoria de threat models previos, papers de investigación, libros de seguridad.

books · research · risks · ai_threats · previous_tms

MODEL TIER HIERARCHY

4 tiers de LLMs

quick

4B params
~3.4 GB VRAM

Parsing · Scoring
DREAD · Validación

stride

9B params
~6.6 GB VRAM

STRIDE · Debate ·
Chain-of-Thought

deep

27B params
~17 GB VRAM

Síntesis · Enriquecimiento
· Deep Thinker

vlm

9B params
~6.6 GB VRAM

Procesamiento de
imágenes · Multimodal

No todas las tareas necesitan el mismo modelo.

THREATX SECURITY

PhiloCyber

Agentic™

Threat modeling que escala

Open source

100% local

Disponible hoy

github.com/philocyber/agent-threat-modeler | philocyber.com

THREATX SECURITY

PhiloCyber