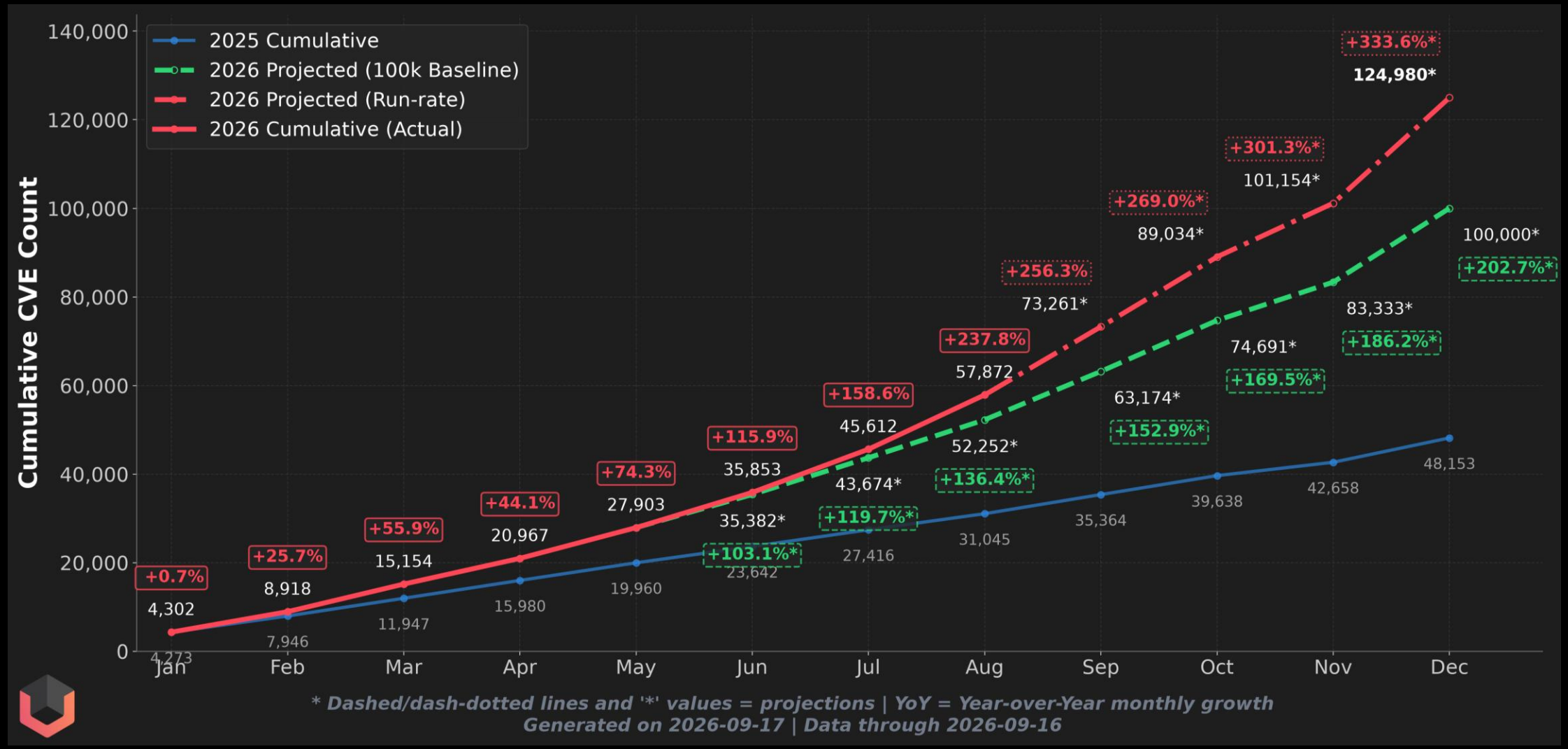
IA de Frontera en Entornos Híbridos, nuevos retos de seguridad

Raúl Guillén –Septiembre 2026

Europe Cybersecurity Strategist

@raulguillen

Publicación acumulada mensual de CVE: 2025 vs. 2026



Fuente: https://alukashenkov.github.io/vulnpocalypse_2026

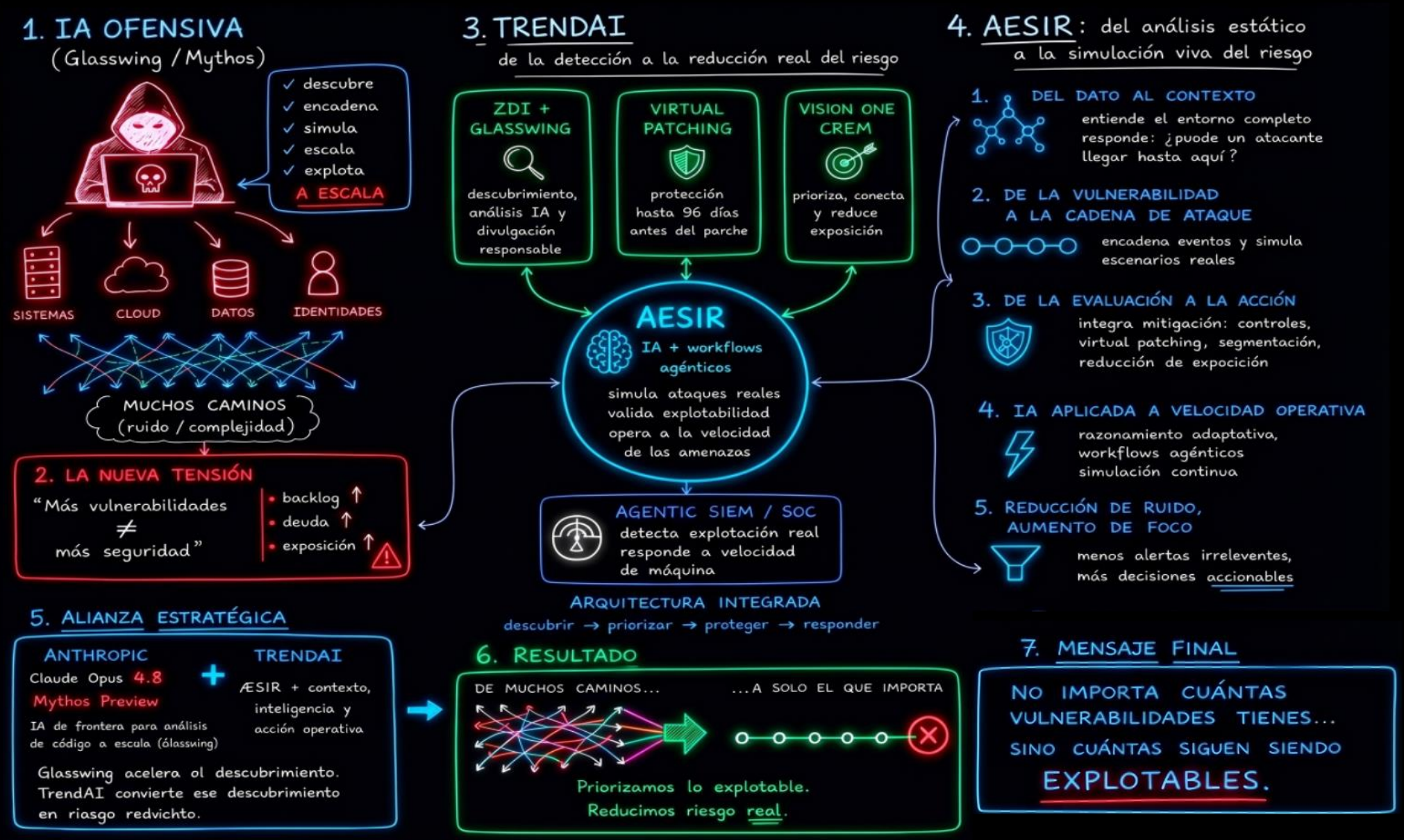
TrendAI

Línea Temporal: IA de Frontera en AAPP 2026.



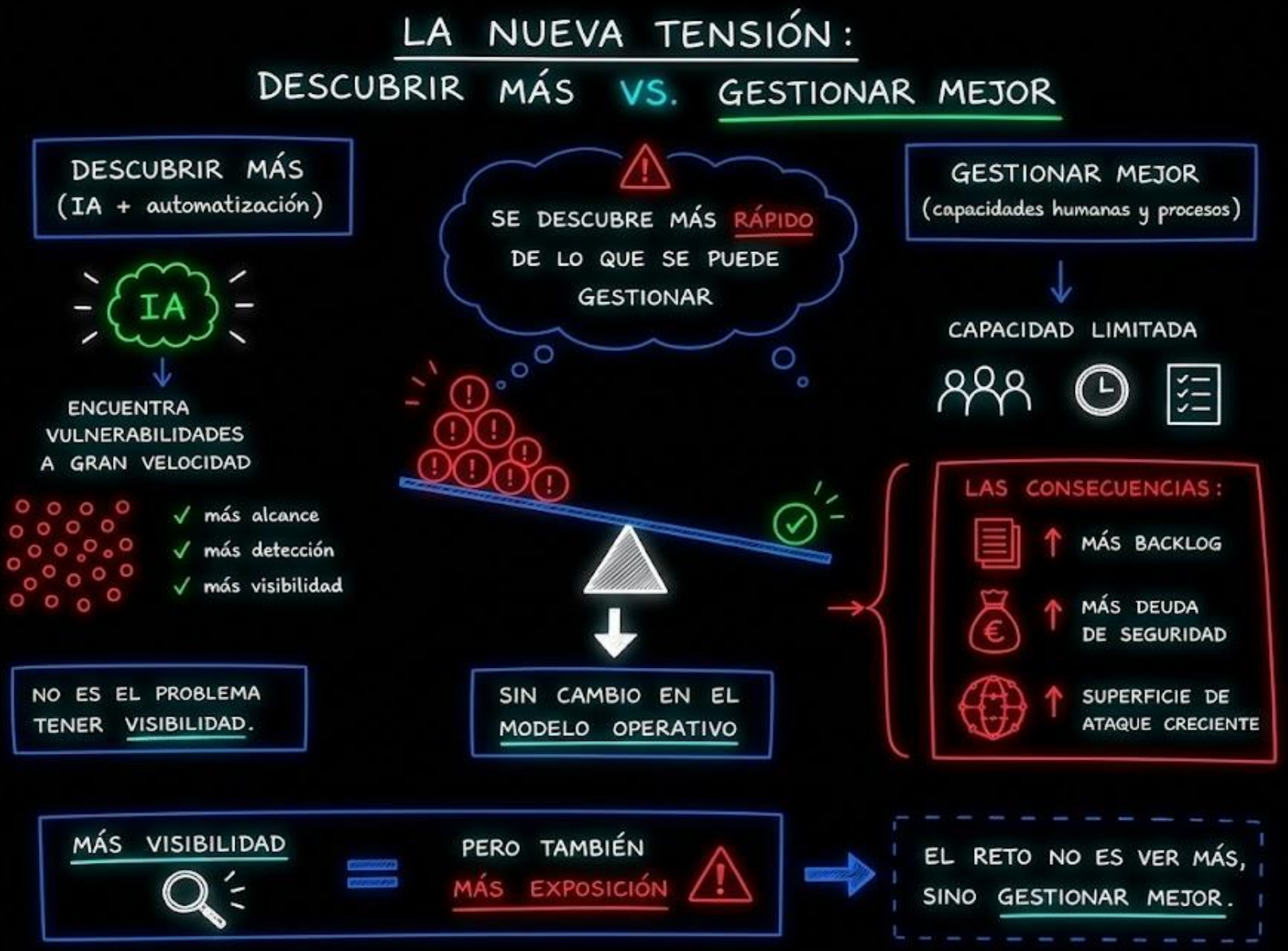
TrendAI™

¿Por qué nos enfrentamos a un cambio de paradigma?



TrendAI

La nueva tensión: descubrir más frente a gestionar mejor



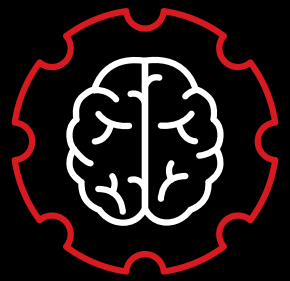
TrendAI™

Sans Institute Framework
3 Dimensiones

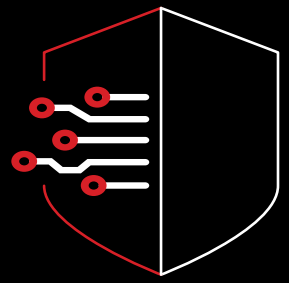
TrendAI™

Sans Institute Framework – 3 Dimensiones

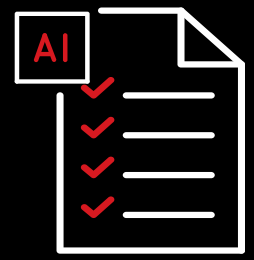
AI & Cybersecurity



AI for Security
(Utilize AI)



Security for AI
(Protect AI)



Govern AI
(Govern AI)

https://sansorg.egnyte.com/dl/XwYQJXyvRpx6



Contexto:

CCN-CERT BP/36 - Junio 2026

Guía de buenas prácticas frente al modelo de IA ofensiva

TrendAI™

Decálogo de recomendaciones

1. Autoevaluación
2. Crear cultura en IA
3. Gobernanza de la IA
4. Cerrar el gap de parcheo
5. Anticiparse a lo que viene
6. Detectar antes de desplegar
7. Revisar lo que ya está en producción
8. Diseñar asumiendo compromiso
9. Gestionar la superficie de ataque
10. Reducir tiempos de respuesta

Fuente: Guía de buenas prácticas frente al modelo de IA ofensiva (BP/36, pg. 46)

AI for Security
(Utilize AI)

TrendAI™

Agentic Exploit-Remediation Engine (ÆSIR)
Del análisis estático a la simulación viva del riesgo

1 DEL DATO AL CONTEXTO



ENTIENDE EL ENTORNO COMPLETO

¿ PUEDE REALMENTE UN ATACANTE LLEGAR HASTA AQUÍ ?

2 DE LA VULNERABILIDAD A LA CADENA DE ATAQUE



- ACCESO INICIAL
- MOVIMIENTO LATERAL
- ESCALADA DE PRIVILEGIOS
- IMPACTO EN ACTIVOS CRÍTICOS

PRIORIZACIÓN BASADA EN EXPLOTABILIDAD REAL EN CONTEXTO

3 DE LA EVALUACIÓN A LA ACCIÓN



- ✓ CONTROLES COMPENSATORIOS
- ✓ VIRTUAL PATCHING (PROTECCIÓN TEMPRANA)
- ✓ SEGMENTACIÓN DE ACCESOS
- ✓ REDUCCIÓN IMMEDIATA DE EXPOSICIÓN

CIERRA EL GAP: DESCURRIR UN PROBLEMA → SOLUCIONARLO

4 IA APLICADA A VELOCIDAD OPERATIVA



- RAZONAMIENTO ADAPTATIVO
- WORKFLOWS AGÉNTICOS
- SIMULACIÓN CONTINUA

NO ANALIZA UNA FOTO FIJA, TRABAJA SOBRE UN ENTORNO VIVO.

5 REDUCCIÓN DE RUIDO, AUMENTO DE FOCO

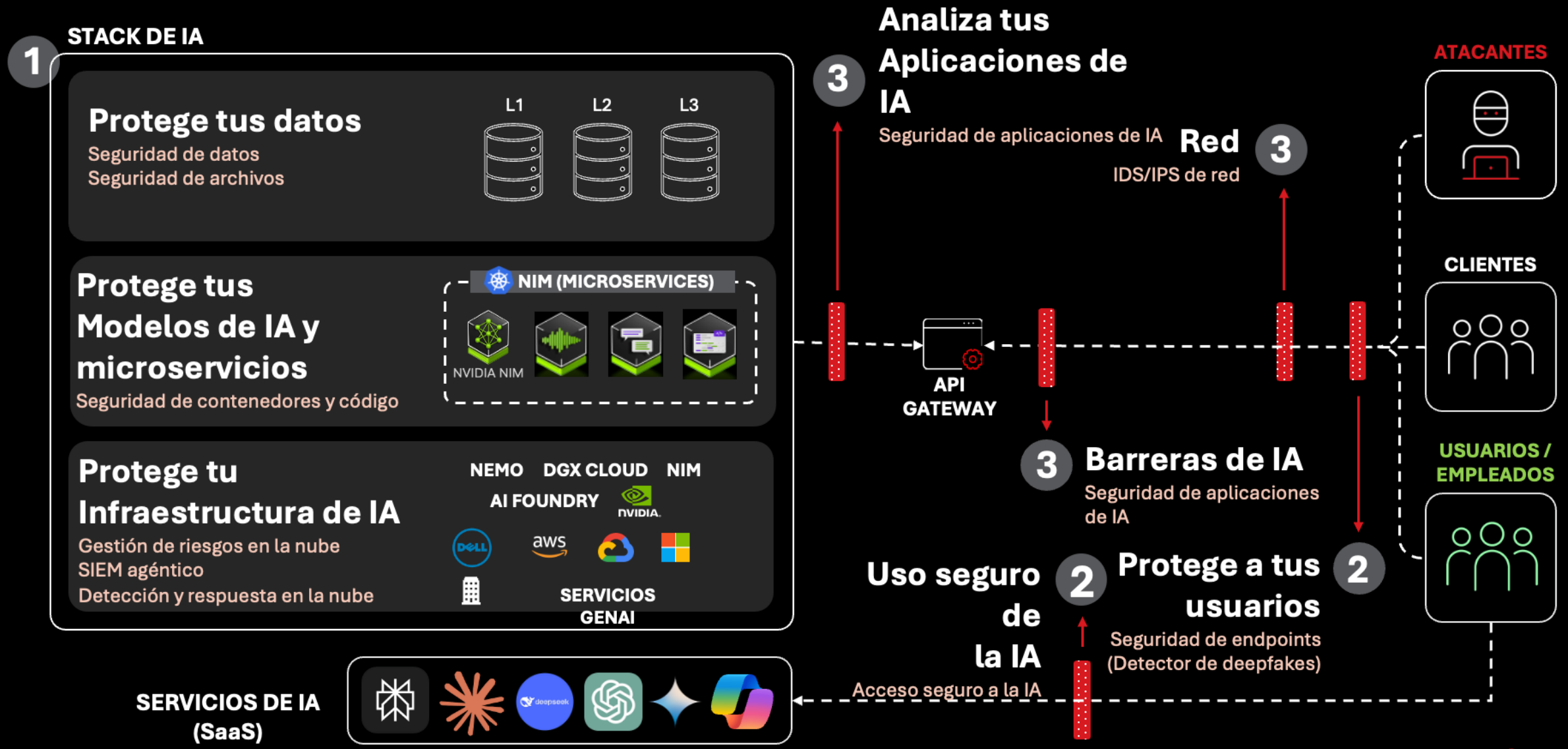


- ✓ MENOS ALERTAS IRRELEVANTES
- ✓ MÁS DECISIONES ACCIONABLES
- ✓ TRADUCE COMPLEZIDAD TÉCNICA EN IMPACTO DE NEGOCIO

MENOS RUIDO, MÁS IMPACTO.

TrendAI

Seguridad de la IA – Esquema



TrendAI

Alianzas estratégicas de IA

NVIDIA

TECNOLOGÍA + GO-TO-MARKET

Seguridad de AI Factory en infraestructura NVIDIA: Vision One EDR con DPU BlueField, además de integraciones NIM y Morpheus.

ANTHROP\C

IA DE FRONTERA + INVESTIGACIÓN DE VULNERABILIDADES + PROYECTO GLASSWING

ÆSIR funciona con Claude Opus 4.8. Participante activo en el Proyecto Glasswing (Claude Mythos Preview).

OpenAI

DAYBREAK CYBER PARTNER

Socio de confianza del programa Daybreak: capacidades cyber de GPT-5.5 integradas en Vision One para detectar y mitigar vulnerabilidades antes de su explotación.

OWASP

ALINEACIÓN CON ESTÁNDARES

Vision One cubre 9 de los 10 riesgos del OWASP Top 10 para LLM. Publicación conjunta de 2025 sobre la protección de la IA generativa.

MITRE ATLAS

MARCO DE INTELIGENCIA DE AMENAZAS

Presentó el primer caso de estudio de MITRE ATLAS sobre ataques de nube/contenedor contra infraestructura de IA. Colaborador activo en el marco de amenazas de IA adversaria.

CoSAI

COALICIÓN DEL SECTOR, PATROCINADOR DESDE 2024

Colaborador en cuatro líneas de trabajo: cadena de suministro de IA, IA agéntica, confianza cero para IA y seguridad de MCP.

TrendAI colabora con los principales proveedores de nube: AWS, Azure y GCP para proteger tanto la infraestructura como los servicios de IA que se ejecutan en ella.


TrendAI
The
AI Security
Playbook for the
New Frontier
Eliminate risk. Prove governance.
Keep operations moving at AI speed.

«La única m

sino cuánta

preparació

Raúl Guillén, E



TrendAI


TrendAI™
AI Fearlessly