Tunich

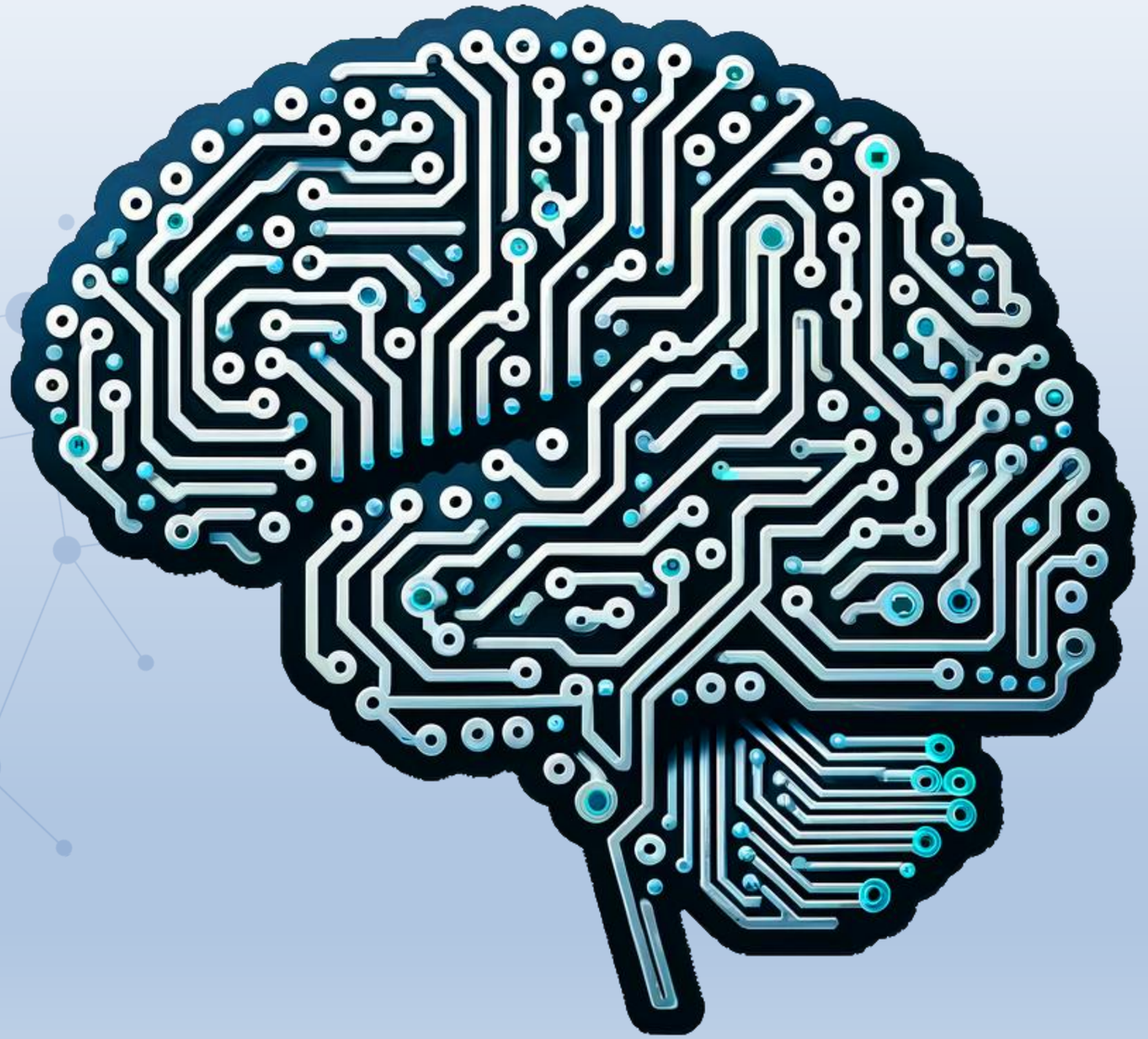
Folleto

TSSC.MX

Tunich

Automatización Inteligente para el Triage y Enriquecimiento de Tickets de Ciberseguridad.

Potencie a su equipo del Centro de Operaciones de Seguridad (SOC) con un motor de IA privado que transforma alertas en análisis accionables, alineados con los marcos de referencia globales en tiempo récord.



El Desafío: Sobrecarga de Alertas y Fricción Operativa

Los directores de TI y seguridad enfrentan una paradoja crítica: más herramientas generan más alertas, pero los equipos humanos no escalan. Esto resulta en:

FATIGA DE ALERTAS
Analistas saturados revisando falsos positivos.

TIEMPO DE RESPUESTA LENTO
La triage manual y la investigación inicial consumen más del 50% del tiempo crítico.

CONOCIMIENTO FRAGMENTADO
Dificultad para alinear incidentes con marcos como MITRE ATT&CK, NIST o ISO 27001 de forma consistente.

RIESGO DE FUGA
La rotación del personal lleva consigo conocimiento tácito valioso.

Nuestra Solución: Un Copiloto de IA para su SOC

SOC Assistant AI es una plataforma de software on-premise que implementa un Modelo de Lenguaje (LLM) especializado de forma segura dentro de su infraestructura. Actúa como un analista junior automatizado que trabaja 24/7, realizando el primer análisis de cada ticket.

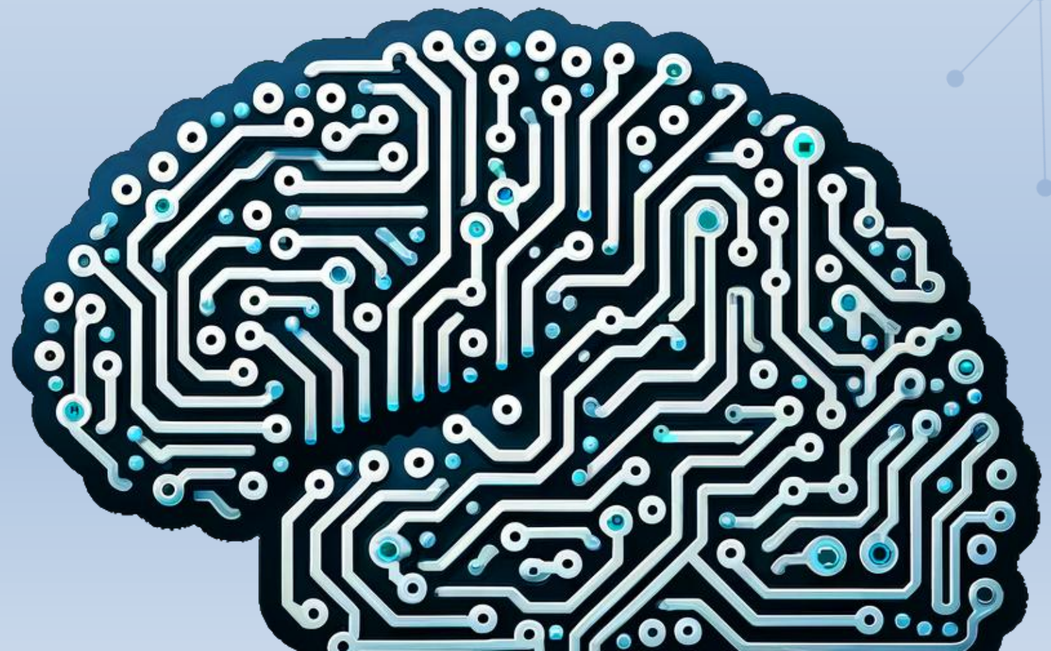
MITRE | ATT&CK®

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

ISO 27002

¿Cómo lo hace?

1. Ingesta Automática: Conecta con sus fuentes de tickets (email, API, SIEM).
2. Análisis y Consulta en Tiempo Real: El LLM extrae entidades clave y consulta automáticamente una base de conocimiento unificada con los marcos MITRE ATT&CK, NIST CSF e ISO 27001.
3. Generación de Ticket Enriquecido: Produce un ticket consolidado con:
    - Clasificación y Contexto claros.
    - Nivel de Riesgo Calibrado (Basado en contexto y marcos).
    - Mapeo a Marcos de Referencia: Tácticas, técnicas (MITRE), controles (NIST/ISO).
    - Recomendaciones de Mitigación Accionables.



Beneficios Clave para el Director de TI/CISO

• Acelere el Tiempo de Respuesta (MTTR): Reduzca la fase del triage e investigación inicial hasta en un 80%, permitiendo que sus analistas senior se enfoquen en amenazas complejas.

• Estandarice y Escale el Conocimiento: Garantice que cada incidente, sin importar quién lo revise, sea analizado contra los mejores marcos del sector, elevando la calidad y consistencia de sus operaciones.

• Reduzca el Riesgo Operacional: Disminuya la probabilidad de error humano en la clasificación inicial y asegure que ningún ticket pase sin las referencias de cumplimiento y mitigación pertinentes.

• Maximice su Inversión en Personal: Libere a sus talentosos analistas de tareas repetitivas, aumentando su satisfacción y permitiéndoles desarrollar habilidades de caza de amenazas (threat hunting) y respuesta avanzada.

• Privacidad y Soberanía Total de Datos: Todo se ejecuta localmente en sus servidores. Sus datos sensibles de incidentes nunca salen de su red. Cumple con los requisitos regulatorios más estrictos (GDPR, LGPD, etc.).

• Integración sin Fricciones: Se conecta con su stack de seguridad actual mediante APIs. Es un multiplicador de fuerza para sus herramientas existentes (SIEM, SOAR, plataforma de ticketing).

¿Por Qué Nuestra Solución es Diferente?

Característica	Soluciones Genéricas de IA/ML	SOC Assistant AI
Privacidad	A menudo en la nube pública (riesgo de datos).	100% On-Premise / Private Cloud.
Contexto	Análisis genérico de alertas.	Especializado en Ciberseguridad con conocimiento integrado de MITRE, NIST, ISO.
Resultado	Más datos o puntuaciones.	Ticket accionable y enriquecido listo para el flujo de trabajo del SOC.
Implementación	Cajas negras complejas.	Arquitectura abierta y modular, adaptable a sus procesos.

Arquitectura Confiable y Escalable

- Backend en FastAPI (Robusto y rápido).
- Motor de IA (LLM Open-Source) seleccionado para equilibrio entre rendimiento y precisión.
- Base de Datos Vectorial (ChromaDB/Weaviate) para búsqueda semántica en los marcos de conocimiento.
- Frontend Opcional (React) o integración completa vía API con su sistema de ticketing (ServiceNow, Jira, etc.).

Imagine un SOC donde:

✔ Las alertas se clasifican y enriquecen en segundos, no en minutos.

✔ Los reportes de cumplimiento (NIST, ISO) se generan automáticamente desde los tickets.

✔ Su equipo se enfoca en cazar amenazas, no en limpiar datos.
Tunich SOC Assistant AI no es solo una herramienta más; es la evolución natural de su centro de operaciones.

Tunich SOC Assistant AI no es solo una herramienta más; es la evolución natural de su centro de operaciones.