PostecH

Ficha técnica

Tunich

SOC Assistant AI

Producto:	Tunich
Versión de documento:	1.0.0
Tipo de Documento:	Ficha Técnica
Fecha de elaboración:	28 de agosto de 2025
Autor:	Postech

FICHA TÉCNICA

Plataforma de software on-premise para automatización del análisis inicial de tickets de seguridad

Producto:	Tunich SOC Assistant AI
Versión de producto:	1
Tipo de Documento:	Ficha Técnica
Fecha:	20 de julio de 2025
Clasificación:	Comercial
Contacto:	ventas@ postech.us

Tabla de contenido

1. DESCRIPCIÓN GENERAL

Nombre de la Solución: Tunich SOC Assistant AI

Tipo: Plataforma de software on-premise para automatización del análisis inicial de tickets de seguridad

Versión: 1.0 (MVP)

Arquitectura: Modular basada en microservicios en contenedores

Modelo de Licenciamiento: Licencia anual por suscripción (incluye soporte y actualizaciones)

2. OBJETIVO TÉCNICO

Automatizar el proceso de triage y enriquecimiento inicial de tickets de incidentes de seguridad mediante un modelo de lenguaje especializado (LLM) ejecutado localmente, integrando conocimiento de marcos de referencia de ciberseguridad.

3. ARQUITECTURA TÉCNICA

3.1 Diagrama de Componentes

[Fuentes de Tickets] → [API Gateway] → [Orquestador Principal] → [LLM Local] → [Bases de Conocimiento]
(Email, SIEM, API) (FastAPI) (Python/Node.js) (Llama/Mistral/DeepSeek R1) (Vector DB + SQL)
↓
[Generador de Tickets]
↓
[Sistema de Ticketing] o [Frontend Web]

3.2 Componentes Principales

Componente	Tecnología	Descripción
API Gateway	FastAPI (Python)	Punto único de entrada para tickets, gestión de autenticación y rate limiting
Motor de Procesamiento	Python 3.10+	Orquestación del flujo de análisis y gestión de pipelines
Modelo LLM	Llama 3/Mistral (Open Source)	Modelo de lenguaje fine-tuneable para análisis de seguridad
Base de Conocimiento	ChromaDB/Weaviate + PostgreSQL	Almacenamiento vectorial para búsqueda semántica en marcos de referencia
Frontend (Opcional)	React + TypeScript	Interfaz para revisión y ajuste de tickets generados

Componente	Tecnología	Descripción
Orquestación	Docker + Docker Compose	Dockerización y gestión de servicios

4. ESPECIFICACIONES FUNCIONALES

4.1 Capacidades de Procesamiento

- **Ingesta de Tickets:** Soporte para email (IMAP/POP3), API REST, webhooks, y archivos CSV/JSON
- **Análisis Automático:** Extracción de entidades (IPs, dominios, hashes, CVE), clasificación inicial
- **Consultas RAG:** Búsqueda semántica en bases de conocimiento de:
    - MITRE ATT&CK® (Tácticas, Técnicas, Sub-técnicas)
    - NIST Cybersecurity Framework (v1.1 y superiores)
    - ISO/IEC 27001:2022 (Anexo A - Controles)
    - (Opcional) Playbooks internos del SOC
- **Generación de Salida:** Tickets estructurados en JSON con:

json

```
{
  "id": "INC-2024-001",
  "resumen": "Análisis enriquecido",
  "clasificacion": "Malware/Phishing",
  "riesgo": {"nivel": "Alto", "score": 85},
  "marcos": {
    "mitre": ["T1566.001", "T1204.002"],
    "nist": ["PR.AC-4", "DE.CM-1"],
    "iso27001": ["A.8.2", "A.12.6"]
  },
  "mitigaciones": ["Lista de acciones recomendadas"],
  "evidencia": ["Fragmentos relevantes del análisis"]
}
```

4.2 Integraciones

- **Sistemas de Ticketing:** API para ServiceNow, Jira Service Management, Zendesk
- **SIEM:** Compatibilidad con Splunk ES, IBM QRadar, Microsoft Sentinel (vía API)
- **SOAR:** Webhooks para Palo Alto XSOAR, Splunk SOAR, TheHive

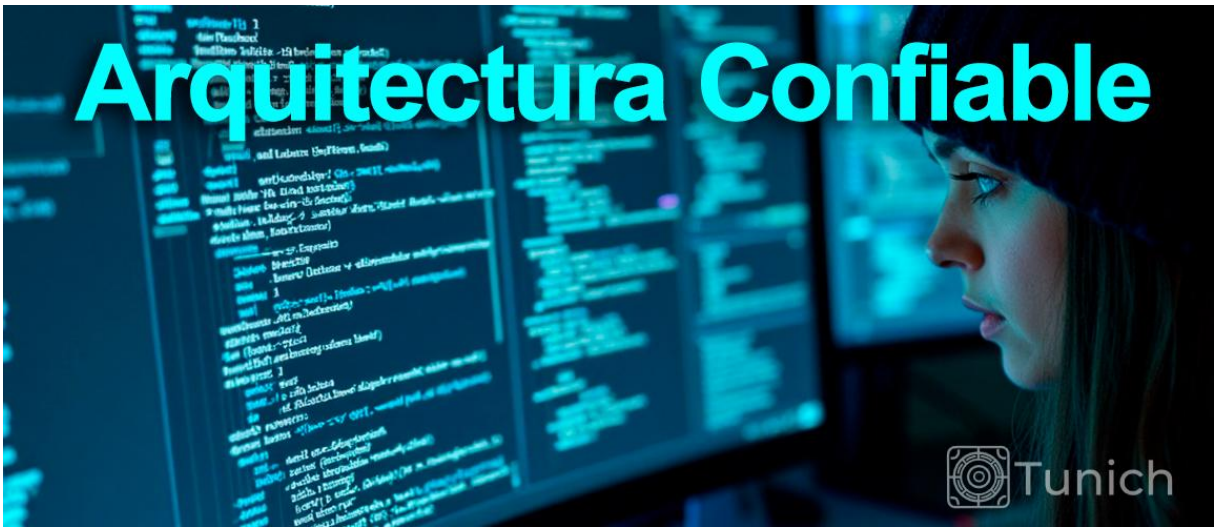
5. REQUISITOS DEL SISTEMA

5.1 Hardware Mínimo

Recurso	Especificación Mínima	Especificación Recomendada
CPU	8 cores modernos (Intel i7/AMD Ryzen 7 o superior)	16+ cores (Xeon/EPYC)
RAM	32 GB DDR4	64+ GB DDR4/DDR5
Almacenamiento	500 GB SSD NVMe	1 TB SSD NVMe (RAID 1 recomendado)
GPU (Opcional)	NVIDIA T4/ (24GB VRAM)	NVIDIA A100/A6000 o 2x RTX 4090 (VRAM 80GB)
Red	1 Gbps Ethernet	10 Gbps para entornos con alto volumen

5.2 Software Base

- **Sistema Operativo:** Ubuntu Server 22.04 LTS / RHEL 9 / Rocky Linux 9
- **Runtime:** Docker Engine 24.0+, Docker Compose 2.20+
- **Dependencias:** NVIDIA Container Toolkit (si se usa GPU), Python 3.10+



6. ESPECIFICACIONES DE SEGURIDAD

6.1 Características de Seguridad

- **Aislamiento:** Todos los componentes corren en contenedores aislados
- **Cifrado:** TLS 1.3 para comunicaciones, cifrado en reposo para datos sensibles
- **Autenticación:** JWT + OAuth2 para APIs, soporte para LDAP/Active Directory
- **Auditoría:** Logs completos de actividades (ingesta, procesamiento, acceso)
- **Sin salida a Internet:** Operación completamente local (air-gap compatible)

6.2 Cumplimiento

- Diseñado para facilitar cumplimiento de:
  - ISO 27001/27002
  - NIST SP 800-53
  - GDPR/LGPD (procesamiento local de datos)
  - Sectoriales (PCI DSS, HIPAA según configuración)

• 7. RENDIMIENTO Y ESCALABILIDAD

7.1 Métricas de Rendimiento

Métrica	Objetivo MVP	Objetivo Escalado
Tickets/hora	100-200	1000+
Latencia por ticket	< 30 segundos	< 10 segundos
Disponibilidad	99.5% (SLA básico)	99.95%
Tiempo de recuperación (RTO)	< 4 horas	< 1 hora

7.2 Estrategias de Escalado

- **Horizontal:** Adición de workers de procesamiento
- **Vertical:** Mejora de recursos GPU/CPU para el modelo LLM
- **Caché:** Implementación de Redis para consultas frecuentes
- **Balanceo de carga:** Para múltiples instancias del motor de análisis

8. IMPLEMENTACIÓN Y MANTENIMIENTO

8.1 Proceso de Implementación

1. **Evaluación (1 semana):** Auditoría de entorno y requisitos específicos
2. **Preparación (1 semana):** Provisionamiento de hardware y configuración base
3. **Despliegue (3 días):** Instalación automatizada vía scripts Ansible
4. **Configuración (1 semana):** Fine-tuning inicial, integraciones, carga de conocimiento
5. **Pruebas (2 semanas):** POC con datos históricos, ajuste de prompts

8.2 Mantenimiento

- **Actualizaciones:** Parches mensuales de seguridad, actualizaciones trimestrales de funcionalidad
- **Backup:** Estrategia incremental diaria + completo semanal
- **Monitoreo:** Dashboards de salud, alertas proactivas, métricas de precisión
- **Soporte:** Niveles Silver/Gold/Platinum (8x5, 16x5, 24x7)

9. ROADMAP TÉCNICO

Fase 1 (MVP - Actual)

- Análisis básico de tickets
- Integración con MITRE ATT&CK y NIST CSF
- Salida en JSON/formatos estructurados

Fase 2 (6 meses)

- Fine-tuning del modelo con datos del cliente
- Integración con SOAR para automatización de respuestas
- Dashboard analítico para métricas del SOC

Fase 3 (12 meses)

- Modelos especializados por tipo de amenaza
- Análisis predictivo de tendencias
- API abierta para desarrolladores internos

10. SOPORTE Y GARANTÍAS

- **Garantía:** 1 año en componentes software
- **SLA de soporte:** Respuesta en < 4 horas para críticos
- **Actualizaciones de conocimiento:** Trimestral para marcos de referencia
- **Documentación:** Completa (administración, API, troubleshooting)
- **Comunidad:** Acceso a portal de clientes con KB y best practices