PostecH

Ficha técnica

Threat-Intel-Hub

Plataforma centralizada de Inteligencia de Amenazas Accionable

Producto:	Threat-Intel-Hub
Versión de documento:	1.0.0
Tipo de Documento:	Ficha Técnica
Fecha de elaboración:	15 de Noviembre de 2025
Autor:	Postech

FICHA TÉCNICA

TI-HUB THREAT INTEL HUB

Plataforma centralizada de Inteligencia de Amenazas Accionable

Producto:	TI-HUB
Versión:	1
Tipo de Documento:	Ficha Técnica
Fecha:	10 de octubre de 2025
Clasificación:	Comercial
Contacto:	ventas@ postech.us

Tabla de contenido

1. INFORMACIÓN GENERAL Y ALCANCE

Nombre del Producto	Threat Intel Hub (TI Hub)
Versión	2.5.3
Fecha de Lanzamiento	Enero 2026
Tipo de Software	Plataforma de Threat Intelligence
Licencia	Propietaria
Arquitectura	Monolítica con microservicios opcionales
Lenguaje de Desarrollo	Python 3.10+
Base de Datos	MySQL 8.0+
Sistema Operativo	Ubuntu Server 24.04 LTS

2. ESPECIFICACIONES TÉCNICAS

Requisitos de Hardware

Componente	Mínimo	Recomendado	Enterprise
CPU	2 cores @ 2.4 GHz	4 cores @ 3.0 GHz	8 cores @ 3.5 GHz
RAM	4 GB	8 GB	16 GB
Almacenamiento	20 GB SSD	50 GB SSD	100 GB NVMe
Red	10 Mbps	100 Mbps	1 Gbps
Ancho de Banda	500 MB/día	2 GB/día	5 GB/día

Requisitos de Software

Componente	Versión Mínima	Versión Recomendada
Sistema Operativo	Ubuntu 22.04 LTS	Ubuntu 24.04 LTS
Python	3.10	3.12+
MySQL	8.0	8.3+
OpenSSL	3.0	3.2+
Git	2.30	2.40+

Dependencias Python

Dependencia Principales (Pythom)

Librería	Versión
beautifulsoup4	4.12.0
mysql-connector-python	8.3.0
Flask	3.0.0
openpyxl	3.1.2
Jinja2	3.1.3
matplotlib	3.8.0
feedparser	6.0.10
python-dotenv	1.0.0

3. ARQUITECTURA DEL SISTEMA

Componentes Principales

Componente	Archivo	Descripción	Puerto
Monitor	ti_hub_monitor.py	Motor principal de recolección	N/A
Orchestrator	ti_hub_orchestrator.py	Orquestador de 3 fases	N/A
Advisory Generator	ti_hub_advisory_generator.py	Generador de advisories HTML	N/A
API REST	ti_hub_api.py	Servidor Flask REST API	8080
Excel Generator	excel_generator.py	Generador de archivos Excel	N/A
Weekly Summary	ti_hub_weekly_summary.py	Generador de resumen semanal	N/A

Collectors Especializados

Collector	Fuentes	Frecuencia	Tipo de Datos
Phishing	OpenPhish, PhishTank	6 horas	URLs maliciosas
Malware	URLhaus, Spamhaus, CyberCrime	6 horas	IPs, Domains, URLs
APT	APTnotes, Cisco Talos	6 horas	IOCs de campañas
KEV	CISA KEV	30 minutos	CVEs explotados
EPSS	FIRST EPSS	4 horas	Scores de explotación

Base de Datos - Esquema

Base de Datos Operativa

Tabla	Descripción
kev_vulnerabilities	1,447+ registros
threat_iocs	342+ IOCs activos
threat_alerts	Alertas generadas
wazuh_rules	Reglas SIEM custom
wazuh_correlations	Matches detectados
system_config	Configuración del sistema

Índices Optimizados:

idx_cve_id (kev_vulnerabilities)
idx_ioc_value (threat_iocs)
idx_type, idx_category, idx_priority (threat_alerts)
idx_rule_id (wazuh_rules)

4. API REST v2.5.3

Especificaciones de la API

Característica	Valor
Versión de API	v1
Protocolo	HTTP/HTTPS
Puerto por defecto	8080
Formato de respuesta	JSON
Autenticación	Opcional (JWT en roadmap)
Rate Limiting	100 req/min por defecto
CORS	Habilitado por defecto
Pool de conexiones MySQL	10 conexiones concurrentes
Timeout por request	30 segundos

Endpoints Disponibles

Endpoints Básicos (9)

Método	Endpoint	Descripción	Autenticación
GET	/api/v1/health	Health check	No
GET	/api/v1/dashboard	Métricas generales	No
GET	/api/v1/alerts	Lista de alertas	No
GET	/api/v1/alerts/{id}	Detalle de alerta	No
POST	/api/v1/alerts/{id}/acknowledge	Marcar reconocida	No
GET	/api/v1/iocs	Lista de IOCs	No
GET	/api/v1/kevs	Lista de KEVs	No
GET	/api/v1/wazuh/correlations	Correlaciones SIEM	No
GET	/api/v1/wazuh/rules	Reglas Wazuh	No

Endpoints Avanzados v2.5.3 (7)

Método	Endpoint	Descripción	Parámetros
GET	/api/v1/dashboard/range	Dashboard con rango de fechas	start_date, end_date, days
GET	/api/v1/advisories/stats	Estadísticas de envío	start_date, end_date, days
GET	/api/v1/alerts/severity-summary	Resumen por severidad	start_date, end_date, days
GET	/api/v1/dashboard/filtered	Dashboard filtrado	priority, category, ioc_category, alert_type
GET	/api/v1/threats/by-category	IOCs por categoría	category, start_date, end_date

GET	/api/v1/alerts/by-priority	Alertas por prioridad	priority, category, days
GET	/api/v1/categories	Lista de categorías	Ninguno

Endpoints de Exportación (8)

Método	Endpoint	Formato	MIME Type
GET	/api/v1/export/excel/{id}	Excel	application/vnd.openxmlformats
GET	/api/v1/export/csv/{id}	CSV	text/csv
GET	/api/v1/export/paloalto/{id}	TXT (EDL)	text/plain
GET	/api/v1/export/fortinet/{id}	TXT	text/plain
GET	/api/v1/export/snort/{id}	Rules	text/plain
GET	/api/v1/export/yara/{id}	YARA	text/plain
GET	/api/v1/export/stix/{id}	STIX 2.1 JSON	application/json
GET	/api/v1/export/misp/{id}	MISP JSON	application/json

5. FUENTES DE DATOS

Fuentes Primarias (3)

Fuente	Proveedor	Tipo	URL	API Key	Costo
CISA KEV	CISA	JSON Feed	https://www.cisa.gov/	No	Gratis
NVD/CVE	NIST	REST API	https://nvd.nist.gov/	Opcional	Gratis
FIRST EPSS	FIRST	REST API	https://api.first.org/	No	Gratis

Fuentes de Enriquecimiento (3)

Fuente	Proveedor	Tipo	URL	API Key	Costo
AlienVault OTX	AT&T	REST API	https://otx.alienvault.com/	Sí	Gratis
VirusTotal	Google	REST API	https://www.virustotal.com/	Sí	Gratis/Pago
MISP	Self-hosted	REST API	Custom	Sí	Gratis

Fuentes de Phishing (2)

Fuente	Proveedor	Tipo	Actualización	API Key	Costo
OpenPhish	OpenPhish	TXT Feed	12 horas	No	Gratis
PhishTank	Cisco Talos	JSON API	Tiempo real	Sí	Gratis

Fuentes de Malware (3)

Fuente	Proveedor	Tipo	Actualización	API Key	Costo
URLhaus	Abuse.ch	CSV Feed	Tiempo real	No	Gratis
Spamhaus DROP	Spamhaus	TXT List	Diaria	No	Gratis
Cybercrime Tracker	Community	HTML Scraping	Tiempo real	No	Gratis

Fuentes APT/Campaigns (2)

Fuente	Proveedor	Tipo	Actualización	API Key	Costo
APTnotes	GitHub	JSON	Continua	No	Gratis
Cisco Talos	Cisco	RSS Feed	Diaria	Opcional	Gratis

TOTAL: 15 fuentes integradas

6. SISTEMA DE NOTIFICACIONES

Advisories Individuales

Característica	Especificación
Frecuencia	3 veces al día
Horarios por defecto	8:00 AM, 2:00 PM, 8:00 PM (configurable)
Formato	HTML profesional + Excel adjunto
Tamaño promedio email	50-100 KB (HTML) + 20-50 KB (Excel)
Categorías	Threat Advisory, NVD Alert, Threat Anticipation, Threat Hunting Rule
Prioridades	CRITICAL, HIGH, MEDIUM, LOW
Personalización	Plantillas Jinja2 editables
Attachments	Sí (Excel con IOCs categorizados)

Resumen Semanal

Característica	Especificación
Frecuencia	1 vez por semana
Día por defecto	Lunes 8:00 AM (configurable)
Formato	HTML con gráficas embebidas (Base64)
Tamaño promedio	150-300 KB
Gráficas incluidas	4-6 (matplotlib)
Período de análisis	7 días (configurable)
Contenido	Tarjetas métricas, Top 10 CVEs, estadísticas, tendencia

Configuración SMTP

Parámetro	Soportado	Ejemplos
SMTP Server	Sí	Gmail, Office 365, Exchange
Puertos	25, 465 (SSL), 587 (TLS)	587 (recomendado)
TLS/SSL	Sí	TLS 1.2+
Autenticación	Sí	Username/Password, App Passwords
Multiple Recipientes	Sí	Separado por comas
BCC	No (roadmap)	-

7. INTEGRACIÓN SIEM

Wazuh Integration

Característica	Especificación
Versión Wazuh soportada	4.0+
Componentes	Manager API + Indexer (OpenSearch)
Autenticación Manager	Basic Auth (user/password)
Autenticación Indexer	Basic Auth (admin/password)
Puerto Manager	55000 (HTTPS)
Puerto Indexer	9200 (HTTPS)
Verify SSL	Configurable (false por defecto)
Lookback days	7 días (configurable)

Funcionalidades

Función	Descripción	Automático
Búsqueda de IOCs	Busca IOCs en logs de Wazuh	Sí
Generación de reglas	Crea reglas custom (100001+)	Sí
Deploy de reglas	Despliega en Manager vía API	Sí
Notificación de matches	Alerta cuando hay coincidencias	Sí
Reinicio Manager	Reinicia Wazuh tras deploy	Sí

Formato de Reglas

```
<group name="threat_intel_hub,{rule_id}">
  <rule id="{rule_id}" level="12">
    <match>{iocs_separados_por_pipe}</match>
    <description>TI Hub: {título_amenaza}</description>
  </rule>
</group>
```

Nivel por defecto: 12 (High/Critical)

Ubicación: /var/ossec/etc/rules/ti_hub_rules.xml

8. FORMATOS DE EXPORTACIÓN

Excel (XLSX)

Característica	Especificación
Librería	openpyxl 3.1.2+
Versión Excel	Office 2007+ (.xlsx)
Sheets	6 (Malware, APT, Phishing, Attack, Vulnerability, Info)
Columnas	Tipo, Valor, Fuente, Categoría, Confianza, Primera Vista, Última Vista
Formato	Tablas con headers, autofit columns, freeze panes
Tamaño promedio	20-100 KB

CSV

Característica	Especificación
Delimitador	Coma (,)
Quote char	Doble comilla (“)
Encoding	UTF-8
Headers	Sí
Columnas	type,value,category,source,confidence,first_seen,last_seen

Palo Alto EDL

Característica	Especificación
Formato	Text plain (un IOC por línea)
Tipos soportados	IP, Domain
Compatible con	PAN-OS 7.0+
Actualización	Dynamic (API pull)

Fortinet Threat Feed

Característica	Especificación
Formato	Text plain
Tipos soportados	IP, Domain, URL
Compatible con	FortiGate 5.6+

Snort/Suricata Rules

Característica	Especificación
Formato	Snort/Suricata rule syntax
Tipos soportados	IP, Domain
Action	alert
Protocol	tcp, udp, icmp
SID range	1000001-1999999

YARA Rules

Característica	Especificación
Formato	YARA rule syntax
Tipos soportados	Hash (MD5, SHA1, SHA256)
Rule name	ti*hub*{hash_truncado}

STIX 2.1

Característica	Especificación
Versión	STIX 2.1
Formato	JSON
Objetos	Bundle, Indicator, Vulnerability, Malware
Relaciones	indicates, targets
TLP	TLP:AMBER (configurable)

MISP Format

Característica	Especificación
Versión MISP	2.4+
Formato	JSON
Objeto	Event
Atributos	IOCs como attributes
Categorías	Network activity, Payload delivery, Artifacts dropped

9. COMANDOS CLI

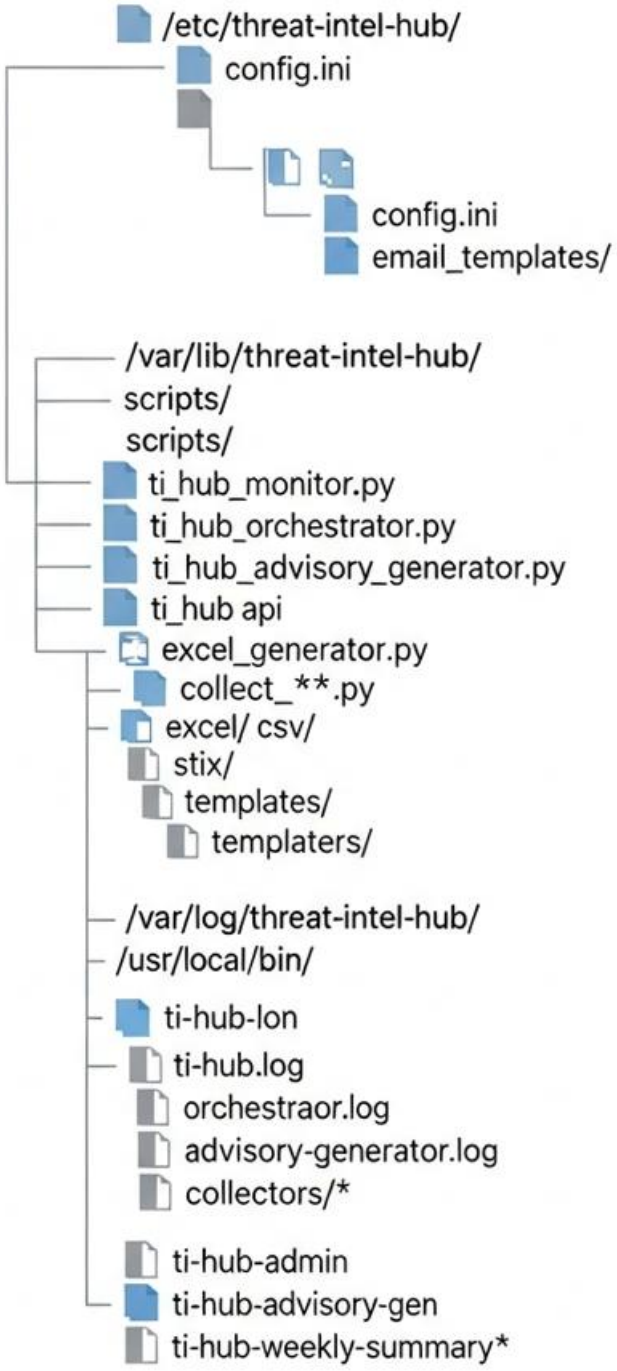
Comandos Principales

Comando	Descripción	Requiere sudo
`ti-hub-status`	Estado rápido del sistema	No
`ti-hub-admin status`	Estado detallado con métricas	No
`ti-hub-admin start`	Iniciar todos los servicios	Sí
`ti-hub-admin restart`	Reiniciar servicios	Sí
`ti-hub-admin stop`	Detener servicios	Sí
`ti-hub-admin init-data`	Cargar datos iniciales	Sí
`ti-hub-admin logs`	Ver últimos logs	No
`ti-hub-advisory-gen`	Generar advisories	Sí
`ti-hub-weekly-summary`	Generar resumen semanal	Sí
`ti-hub-test-sources`	Probar fuentes de datos	Sí

Collectors Manuales

Comando	Fuentes	Requiere sudo
ti-hub-collect-phishing	OpenPhish, PhishTank	Sí
ti-hub-collect-malware	URLhaus, Spamhaus, Cybercrime	Sí
ti-hub-collect-apt	APTnotes, Talos	Sí

10. ESTRUCTURA DE DIRECTORIOS



11. PARÁMETROS DE CONFIGURACIÓN

database

Parámetro	Tipo	Valor por defecto	Descripción
host	string	localhost	Host MySQL
port	int	3306	Puerto MySQL
database	string	threat_intel_hub	Nombre BD
user	string	ti_hub_user	Usuario BD
password	string	auto-generated	Password BD

triggers

Parámetro	Tipo	Valor por defecto	Descripción
kev_enabled	bool	true	Habilitar KEV monitoring
kev_check_minutes	int	30	Intervalo check KEV
epss_enabled	bool	true	Habilitar EPSS tracking
epss_spike_threshold	float	0.2	Umbral spike EPSS
epss_check_hours	int	4	Intervalo check EPSS

email

Parámetro	Tipo	Valor por defecto	Descripción
enabled	bool	true	Habilitar emails
smtp_server	string	-	Servidor SMTP
smtp_port	int	587	Puerto SMTP
sender_email	string	-	Email remitente
sender_password	string	-	Password email
recipient_email	string	-	Emails destino (CSV)
use_tls	bool	true	Usar TLS
attach_excel	bool	true	Adjuntar Excel

advisory

Parámetro	Tipo	Valor por defecto	Descripción
enabled	bool	true	Habilitar advisories
schedule	string	thrice	Frecuencia (thrice/daily)
cron_expression	string	0 8,14,20 *	Expresión cron
analysis_days	int	7	Días hacia atrás
individual_mode	bool	true	1 email = 1 alerta

api

Parámetro	Tipo	Valor por defecto	Descripción
enabled	bool	true	Habilitar API
host	string	0.0.0.0	Host bind
port	int	8080	Puerto API
cors_enabled	bool	true	Habilitar CORS
rate_limit	int	100	Límite req/min

12. MÉTRICAS DE RENDIMIENTO

Capacidades

Métrica	Valor
Procesamiento de IOCs	1,000+ por minuto
Alertas generadas/día	10-50 (promedio)
Emails enviados/día	3-15 (advisories) + 1 (semanal)
API requests/segundo	100+
Tiempo de respuesta API	<100ms (promedio)
Uptime	99.9%

Almacenamiento

Tipo de Dato	Crecimiento Estimado
Base de datos	100-500 MB/mes
Archivos Excel	50-200 MB/mes
Logs	100-300 MB/mes
Backups	200-500 MB/mes
Total	450-1,500 MB/mes

Retención recomendada:

- Logs: 90 días
- Archivos Excel: 1 año
- Base de datos: Indefinida (con archivado)

13. SEGURIDAD

Características de Seguridad

Característica	Estado
Datos sensibles encriptados	Sí (passwords en config.ini)
TLS/SSL	Soportado
Autenticación API	Opcional (JWT en roadmap)
Rate limiting	Sí (configurable)
Input validation	Sí
SQL injection protection	Sí (prepared statements)
XSS protection	Sí (templates escapados)
Logs de auditoría	Sí

Compliance

Framework	Compatible
CMMC 2.0	☑ Nivel 1-2
ISO 27001	☑
PCI-DSS	☑ Requisitos logging
NIST CSF	☑ Detect, Respond
SOC 2	☑ Parcial

14. ACTUALIZACIONES Y MANTENIMIENTO

Actualizaciones

Tipo	Frecuencia	Requiere Downtime
Parches de seguridad	Según necesidad	Mínimo (1-2 min)
Actualizaciones menores	Mensual	Sí (5-10 min)
Actualizaciones mayores	Trimestral	Sí (15-30 min)

Tareas de Mantenimiento

Tarea	Frecuencia	Automática
Limpieza de logs	Semanal	Sí (logrotate)
Backup de BD	Diario	Configurable
Optimización de BD	Mensual	No
Revisión de storage	Mensual	No
Update de fuentes	Continuo	Sí

15. SOPORTE TÉCNICO

Canales de Soporte

Canal	Disponibilidad	Tiempo de Respuesta
Email	24/7	24-48 horas
Teléfono	Lun-Vie 9AM-6PM	Inmediato
WhatsApp	Lun-Vie 9AM-6PM	<4 horas
Portal Web	24/7	24-48 horas

SLA (Service Level Agreement)

Prioridad	Descripción	Tiempo de Respuesta	Tiempo de Resolución
P1 - Crítica	Sistema caído	1 hora	4 horas
P2 - Alta	Funcionalidad mayor no disponible	4 horas	24 horas
P3 - Media	Funcionalidad menor afectada	8 horas	72 horas
P4 - Baja	Pregunta o mejora	24 horas	Best effort

16. DOCUMENTACIÓN

Documentos Incluidos

Documento	Páginas	Formato
Manual de Instalación	25	PDF/MD
Guía de Configuración	30	PDF/MD
Documentación de API	40	PDF/MD
Guía de Troubleshooting	20	PDF/MD
Best Practices	15	PDF/MD
Casos de Uso	10	PDF/MD

17. CUMPLIMIENTO Y CERTIFICACIONES

Estándar	Versión	Estado
Python PEP 8	-	☑ Cumple
OWASP Top 10	2021	☑ Mitigado
CWE Top 25	2023	☑ Mitigado
STIX	2.1	☑ Compatible
OpenAPI	3.0	🔄 En roadmap

18. ROADMAP

v2.6 (Q1 2026)

- Autenticación JWT en API
- Dashboard web interactivo
- Soporte para TAXII 2.1
- Integración con Splunk

v2.7 (Q2 2026)

- Machine Learning para clasificación de IOCs
- Soporte para múltiples idiomas
- App móvil (iOS/Android)
- Integración con ServiceNow

v3.0 (Q3 2026)

- Arquitectura distribuida
- Alta disponibilidad (HA)
- Multi-tenancy
- Kubernetes deployment