PostecH

THREAT INTEL HUB

FOLLETO

POSTECH.US

THREAT INTEL HUB

Threat Intel Hub (TI Hub) es una plataforma integral de inteligencia de amenazas cibernéticas que automatiza la recolección, enriquecimiento, correlación y distribución de información de seguridad desde múltiples fuentes globales. La solución está diseñada para Centros de Operaciones de Seguridad (SOC) y equipos de respuesta a incidentes que requieren inteligencia accionable en tiempo real.

PROPUESTA DE VALOR

- **Automatización completa**
- **Fuentes de inteligencia integradas**
- **Integración SIEM nativa**
- **Sistema de notificaciones multi-nivel**
- **API REST completa**
- **Exportación multi-formato**

FUNCIONALIDADES

MÓDULO DE RECOLECCIÓN

- ✓ INTEGRACIÓN CON 15+ FUENTES DE INTELIGENCIA
- ✓ COLLECTORS ESPECIALIZADOS (PHISHING, MALWARE, APT)
- ✓ MONITOREO CONTINUO 24/7
- ✓ DEDUPLICACIÓN AUTOMÁTICA DE DATOS
- ✓ MANEJO DE RATE LIMITS Y ERRORES

MÓDULO DE ENRIQUECIMIENTO

- ✓ INTEGRACIÓN ALIENVAULT OTX
- ✓ INTEGRACIÓN VIRUSTOTAL
- ✓ INTEGRACIÓN MISP (OPCIONAL)
- ✓ CATEGORIZACIÓN AUTOMÁTICA DE IoCs
- ✓ ANÁLISIS DE PROBABILIDAD EPSS

MÓDULO DE CORRELACIÓN

- ✓ INTEGRACIÓN WAZUH SIEM
- ✓ BÚSQUEDA AUTOMÁTICA EN LOGS (7 DÍAS)
- ✓ GENERACIÓN DE REGLAS CUSTOM
- ✓ AUTO-DEPLOY DE REGLAS
- ✓ NOTIFICACIÓN DE COINCIDENCIAS

MÓDULO DE DISTRIBUCIÓN

- ✓ ADVISORIES INDIVIDUALES (HTML + EXCEL)
- ✓ RESUMEN SEMANAL CON GRÁFICAS
- ✓ 4 TIPOS DE NOTIFICACIÓN
- ✓ PERSONALIZACIÓN DE TEMPLATES
- ✓ MÚLTIPLES DESTINATARIOS

API REST

- ✓ 9 ENDPOINTS BÁSICOS
- ✓ 7 ENDPOINTS AVANZADOS (V2.5.3)
- ✓ 8 FORMATOS DE EXPORTACIÓN
- ✓ DOCUMENTACIÓN COMPLETA
- ✓ POOL DE CONEXIONES MYSQL

COMANDOS ADMINISTRATIVOS

- ✓ 12+ COMANDOS CLI
- ✓ GESTIÓN DE SERVICIOS
- ✓ TESTING DE FUENTES
- ✓ GENERACIÓN MANUAL DE REPORTES
- ✓ LOGS CENTRALIZADOS

BASE DE DATOS

- ✓ MYSQL 8.0+ OPTIMIZADO
- ✓ 5 TABLAS PRINCIPALES
- ✓ ÍNDICES OPTIMIZADOS
- ✓ PROCEDIMIENTOS ALMACENADOS
- ✓ BACKUPS AUTOMÁTICOS

BENEFICIOS CLAVE

80%

REDUCCIÓN EN TIEMPO DE ANÁLISIS

$108K

AHORRO ANUAL ESTIMADO

15+

FUENTES INTEGRADAS EN UNA PLATAFORMA

<24

HORAS PARA IMPLEMENTACIÓN COMPLETA

99.9%

UPTIME OBJETIVO

GRACIAS

ventas@postech.us