Ficha técnica
CTH

Plataforma MDR Integral de Ciberseguridad

Producto:	Cyber Threat Hunter
Versión de documento:	1.0.0
Tipo de Documento:	Ficha Técnica
Fecha de elaboración:	1 de septiembre de 2025
Autor:	Postech

FICHA TÉCNICA

Plataforma de Managed Detection and Response (MDR)

Producto:	Cyber Threath Hunter (CTH)
Versión de producto:	1.1
Tipo de Documento:	Ficha Técnica
Fecha:	11 de agosto de 2025
Clasificación:	Comercial
Contacto:	ventas@postech.us

Tabla de contenido

1. Información General del Producto

1.1 Identificación de la Solución

Atributo	Especificación
Nombre del Producto	Cyber Threat Hunter (CTH)
Versión Actual	0.02
Fabricante	Postech
Tipo de Solución	Managed Detection and Response (MDR) / SIEM
SOC Operador	Teliko SOC
Sitio Web	www.postech.us
ID de Sistema	7987456321

1.2 Descripción General

Cyber Threat Hunter (CTH) es una plataforma integral de Managed Detection and Response (MDR) que combina capacidades avanzadas de SIEM, SOAR, Threat Intelligence y User Behavior Analytics en una solución unificada. Diseñada para proporcionar detección, análisis y respuesta a amenazas cibernéticas en tiempo real, CTH permite a las organizaciones elevar significativamente su postura de seguridad sin la necesidad de construir y mantener un SOC interno completo.

La plataforma integra múltiples motores de análisis incluyendo correlación de eventos, análisis de comportamiento (UEBA), machine learning y threat intelligence de más de 209,000 indicadores de compromiso (IOCs) activos, proporcionando una defensa en profundidad contra amenazas conocidas y desconocidas.

1.3 Problema que Resuelve

Sobrecarga de Alertas: Reduce la fatiga de alertas mediante triage automatizado y priorización inteligente basada en contexto y criticidad de activos.

Escasez de Talento: Proporciona acceso a un equipo de analistas especializados 24/7 sin necesidad de contratación y retención de personal interno.

Tiempo de Respuesta: Automatiza acciones de contención para reducir el MTTR de horas a minutos.

Visibilidad Fragmentada: Unifica datos de múltiples fuentes de seguridad en una vista consolidada.

1.4 Propuesta de Valor

Pilares de Seguridad Cubiertos

Pilar	Cobertura	Mecanismos
Confidencialidad	Alta	Cifrado TLS 1.2+, AES-256, control de acceso RBAC, MFA
Integridad	Alta	Validación de logs, checksums, auditoría de cambios
Disponibilidad	Alta	Arquitectura HA, monitoreo 24/7, SLA 99.9%

Beneficios Principales

BENEFICIOS CLAVE
✓ Reducción del 80% en tiempo de investigación inicial
✓ Contención automatizada de amenazas en menos de 5 minutos
✓ Cumplimiento de SLA superior al 99%
✓ Visibilidad unificada de toda la infraestructura de seguridad
✓ Acceso a equipo de analistas especializados 24/7/365
✓ Reducción significativa del costo total de operación del SOC
✓ Mapeo automático a frameworks MITRE ATT&CK, NIST, ISO 27001

2. Funcionalidades Principales

2.1 Monitoreo en Tiempo Real

CTH proporciona vigilancia continua 24/7/365 de la infraestructura de TI del cliente, incluyendo redes, servidores, endpoints, aplicaciones y servicios en la nube. El monitoreo es ejecutado por el equipo del Teliko SOC, respaldado por automatización inteligente.

Capacidad	Descripción
Cobertura de Activos	Servidores (Windows/Linux), endpoints, firewalls, switches, aplicaciones, cloud
Frecuencia de Polling	Tiempo real (streaming) + polling cada 5 minutos para reconciliación
Métricas Monitoreadas	Eventos de seguridad, rendimiento, disponibilidad, comportamiento de usuarios
Dashboards	Ejecutivo (alto nivel) y Operacional (detalle técnico)
Alertas en Tiempo Real	Notificaciones inmediatas por severidad vía email, SMS, webhook

2.2 Detección de Amenazas

CTH utiliza múltiples motores de detección que trabajan en conjunto para identificar amenazas conocidas y desconocidas:

Motor	Tecnología	Cobertura
Correlación de Eventos	Reglas SIGMA, correlación multi-fuente	Patrones de ataque conocidos, TTPs
Threat Intelligence	209,565+ IOCs activos de 12+ fuentes	IPs maliciosas, dominios, hashes, URLs
UEBA	Análisis de comportamiento con ML	Amenazas internas, cuentas comprometidas
Machine Learning	Modelos supervisados y no supervisados	DGA, exfiltración, movimiento lateral
Firmas/Signatures	Base de datos actualizada diariamente	Malware conocido, exploits, vulnerabilidades

Tipos de Amenazas Detectadas

AMENAZAS CUBIERTAS
✓ Ransomware y malware avanzado
✓ Phishing y spear-phishing
✓ Ataques de fuerza bruta y credential stuffing
✓ Movimiento lateral y escalación de privilegios
✓ Exfiltración de datos
✓ Amenazas internas (insider threats)
✓ Comunicación con C2 (Command & Control)
✓ Explotación de vulnerabilidades conocidas (CVE)
✓ Ataques DDoS y de denegación de servicio

2.3 Gestión de Logs y Eventos

CTH recopila, normaliza, enriquece y almacena eventos de seguridad de múltiples fuentes, proporcionando una vista unificada para análisis forense e investigación de incidentes.

Característica	Especificación
Fuentes Soportadas	Firewalls, IDS/IPS, EDR, AD, servidores, aplicaciones, cloud, bases de datos
Protocolos de Ingesta	Syslog (UDP/TCP/TLS), API REST, Beats, Kafka, webhooks
Normalización	Parsing automático con soporte para formatos CEF, LEEF, JSON, XML
Enriquecimiento	GeoIP, threat intelligence, contexto de activos, información de usuarios
Retención	Configurable: 30, 90, 180, 365 días según requisitos de cumplimiento
Búsqueda	Motor Elasticsearch con queries en tiempo real y búsqueda histórica
Volumen	Escalable según necesidades (desde 1 GB/día hasta 100+ TB/día)

2.4 Alertas y Reportes

Sistema de Alertas

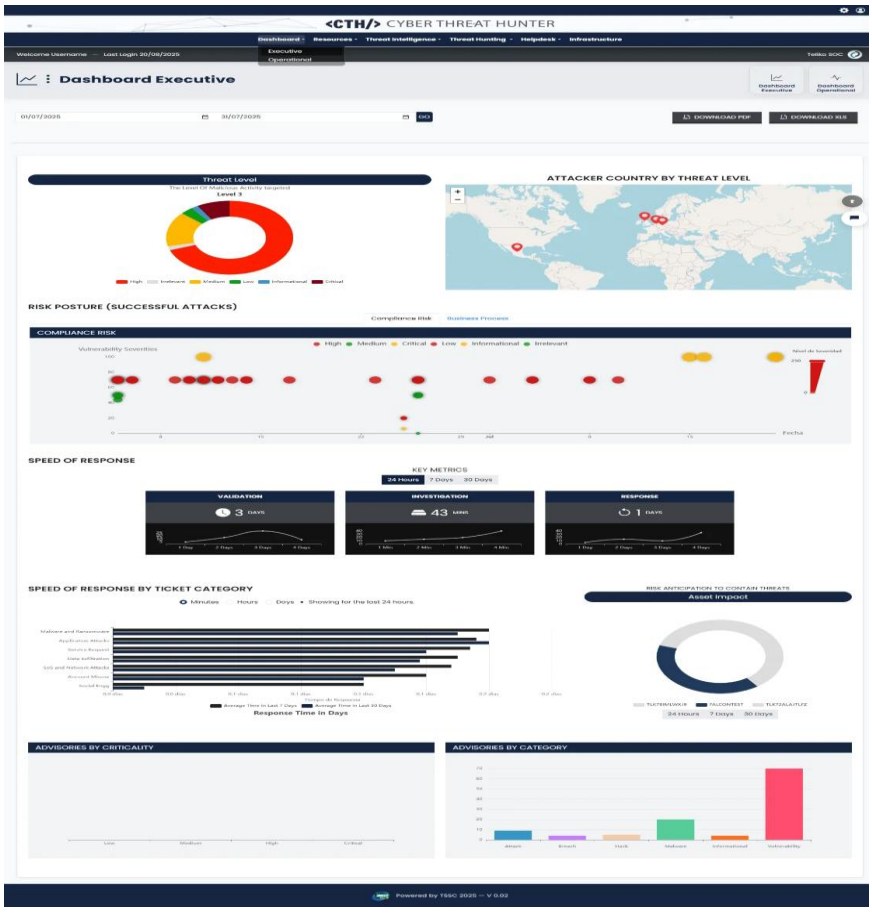
Severidad	Tiempo de Validación	Tiempo de Respuesta	Canales de Notificación
Critical	15 minutos	Inmediato (Automático)	Email, SMS, Llamada, Webhook
High	30 minutos	< 1 hora	Email, SMS, Webhook
Medium	60 minutos	< 4 horas	Email, Webhook
Low	4 horas	< 24 horas	Email, Dashboard

Reportes Disponibles

Reporte	Frecuencia	Contenido
Ejecutivo Mensual	Mensual	KPIs, tendencias, recomendaciones estratégicas
Operacional Semanal	Semanal	Incidentes, tiempos de respuesta, excepciones SLA
Cumplimiento	Bajo demanda	Mapeo a ISO 27001, NIST CSF, PCI-DSS
Threat Intelligence	Diario	IOCs relevantes, campañas activas, advisories
Vulnerabilidades	Semanal	CVEs detectados, priorización, remediación

2.5 Visualización (Dashboard)

CTH proporciona dashboards interactivos diseñados para diferentes audiencias y necesidades operativas:



Dashboard	Audiencia	Métricas Principales
Ejecutivo	CISO, CIO, Dirección	Nivel de amenaza, postura de riesgo, cumplimiento SLA, tendencias
Operacional	Analistas SOC	Alertas activas, tickets, investigaciones, eventos por fuente
Threat Intelligence	Threat Hunters	IOCs activos, matches, advisories, activos impactados
Vulnerabilidades	Equipo de Seguridad	CVEs por severidad, activos afectados, remediación
Helpdesk	Service Desk	Tickets abiertos, SLA compliance, tiempos de respuesta

3. Requisitos Técnicos y Arquitectura

3.1 Plataforma de Despliegue

Modelo	Descripción	Caso de Uso
On-Premise	Instalación completa en infraestructura del cliente	Máxima soberanía de datos, regulaciones estrictas
Nube Privada	Despliegue en nube dedicada del cliente	Escalabilidad con control de datos
Híbrido	Datos sensibles on-premise, procesamiento en nube	Balance entre control y flexibilidad
SaaS (Roadmap)	Servicio completamente gestionado por Postech	Organizaciones sin infraestructura dedicada

3.2 Requisitos del Sistema

Servidor Principal (All-in-One)

Componente	Mínimo	Recomendado	Enterprise
CPU	8 cores	16 cores	32+ cores
RAM	32 GB	64 GB	128+ GB
Almacenamiento	500 GB SSD	2 TB NVMe	10+ TB NVMe RAID
Red	1 Gbps	10 Gbps	10 Gbps redundante
Sistema Operativo	Ubuntu 22.04 LTS	Ubuntu 24.04 LTS	Ubuntu 24.04 LTS
Eventos/Segundo	Hasta 1,000 EPS	Hasta 10,000 EPS	50,000+ EPS

Base de Datos

Componente	Especificación
Motor Principal	PostgreSQL 14+ / MariaDB 10.6+
Motor de Búsqueda	Elasticsearch 8.x
Cache	Redis 7.x
Cola de Mensajes	RabbitMQ 3.12+
Almacenamiento Requerido	Mínimo 1 TB para retención de 90 días (variable según volumen)

3.3 Compatibilidad

Sistemas Operativos Soportados (Fuentes de Datos)

Sistema Operativo	Versiones
Windows Server	2016, 2019, 2022
Windows Desktop	10, 11
Linux (RHEL/CentOS)	7, 8, 9
Linux (Ubuntu)	20.04 LTS, 22.04 LTS, 24.04 LTS
Linux (Debian)	10, 11, 12
macOS	11 (Big Sur) y posteriores

Dispositivos de Red y Seguridad

Categoría	Fabricantes/Productos Soportados
Firewalls	Palo Alto Networks, Fortinet, Check Point, Cisco ASA/Firepower, pfSense
EDR/XDR	CrowdStrike Falcon, Microsoft Defender, SentinelOne, Cytomic EPDR, Cortex XDR
IDS/IPS	Snort, Suricata, Cisco IPS, Palo Alto Threat Prevention
Switches/Routers	Cisco, Juniper, Arista, HP/Aruba
WAF	Imperva, Cloudflare, AWS WAF, F5
Cloud	AWS (CloudTrail, GuardDuty), Azure (Sentinel), GCP (Security Command Center)
ITSM	ServiceNow, Jira Service Management

3.4 Arquitectura de Alto Nivel

La arquitectura de CTH sigue un modelo de capas que garantiza escalabilidad, modularidad y alta disponibilidad:

Capa	Componentes	Función
Ingesta	Colectores, Beats, Syslog, APIs	Recepción y normalización de datos
Procesamiento	Correlación, UEBA, ML, TI Engine	Análisis y detección de amenazas
Almacenamiento	PostgreSQL, Elasticsearch, Redis	Persistencia y búsqueda de datos
Orquestación	RabbitMQ, Workers, Playbooks	Automatización de respuesta
Presentación	React Dashboard, API REST	Interfaz de usuario y integraciones
Gestión	Docker/K8s, Monitoring, Backup	Operación y mantenimiento

4. Seguridad y Cumplimiento

4.1 Certificaciones y Frameworks

CTH está diseñado para facilitar el cumplimiento de los principales marcos regulatorios y estándares de la industria:

Certificación/Framework	Estado	Cobertura
ISO 27001	Compatible	Mapeo de controles de seguridad de la información
NIST Cybersecurity Framework	Compatible	Funciones: Identify, Protect, Detect, Respond, Recover
MITRE ATT&CK	Integrado	Mapeo de TTPs en detecciones y advisories
PCI-DSS	Compatible	Requisitos de logging, monitoreo y respuesta a incidentes
GDPR	Compatible	Protección de datos personales, notificación de brechas
LFPDPPP (México)	Compatible	Cumplimiento de protección de datos personales
SOC 2 Type II	En proceso	Controles de seguridad, disponibilidad y confidencialidad

4.2 Protección de la Plataforma

Cifrado de Datos

Tipo	Algoritmo	Aplicación
En Tránsito	TLS 1.2 / TLS 1.3	Todas las comunicaciones entre componentes y con usuarios
En Reposo	AES-256	Base de datos, logs almacenados, backups
Credenciales	Argon2 / bcrypt	Contraseñas de usuarios y cuentas de servicio
API Keys	SHA-256 HMAC	Tokens de autenticación de integraciones

Control de Acceso

Mecanismo	Descripción
RBAC	Control de acceso basado en roles (Administrator, Manager, TMDR, Engineer, Analyst)
MFA	Autenticación multifactor obligatoria para acceso administrativo
SSO	Integración con proveedores de identidad (SAML 2.0, OAuth 2.0, LDAP/AD)
Auditoría	Registro completo de todas las acciones de usuarios
Sesiones	Timeout configurable, invalidación de sesiones, control de sesiones concurrentes

Seguridad de la Infraestructura

CONTROLES DE SEGURIDAD
✓ Hardening de sistema operativo según CIS Benchmarks
✓ Firewall de host con reglas restrictivas (deny by default)
✓ Actualizaciones de seguridad automatizadas
✓ Escaneo de vulnerabilidades periódico de la plataforma
✓ Segregación de red para componentes críticos
✓ Backups cifrados con verificación de integridad
✓ Monitoreo de integridad de archivos (FIM)
✓ Logs de auditoría inmutables

5. Soporte y Servicios

5.1 Modelo de Soporte

Nivel	Disponibilidad	Tiempo de Respuesta	Canales
Crítico (P1)	24/7/365	15 minutos	Teléfono, Email, WhatsApp
Alto (P2)	24/7/365	1 hora	Teléfono, Email, WhatsApp
Medio (P3)	Lunes a Viernes 8-20h	4 horas	Email, Portal
Bajo (P4)	Lunes a Viernes 9-18h	24 horas	Email, Portal

5.2 Servicios Incluidos

SERVICIOS MDR INCLUIDOS
✓ Monitoreo 24/7/365 por analistas especializados
✓ Triaje y validación de alertas
✓ Investigación de incidentes de seguridad
✓ Contención automatizada de amenazas
✓ Threat hunting proactivo
✓ Reportes ejecutivos y operacionales
✓ Soporte técnico para la plataforma
✓ Actualizaciones de reglas y threat intelligence
✓ Revisiones de seguridad trimestrales

5.3 Modelo de Licenciamiento

Modelo	Base de Cálculo	Incluye
Por Activos	Número de endpoints/servidores monitoreados	Agentes, monitoreo, respuesta
Por Volumen	GB/día de logs ingeridos	Almacenamiento, procesamiento, retención
Por Usuario	Usuarios con acceso a la plataforma	Licencias de consola, dashboards
Enterprise	Paquete integral (activos + volumen ilimitado)	Todo incluido + servicios premium

El licenciamiento es anual con opciones de pago mensual o anual anticipado. Los servicios MDR del Teliko SOC están incluidos en todos los modelos de licenciamiento.

5.4 SLAs Garantizados

Métrica	Objetivo	Penalización por Incumplimiento
Disponibilidad de Plataforma	99.9%	Créditos de servicio proporcionales
Tiempo de Validación de Alertas	Según severidad (15-240 min)	Extensión de contrato
Tiempo de Contención	Automático / < 30 min	Revisión de cuenta
SLA Compliance General	> 99%	Descuentos en renovación

6. Casos de Uso

6.1 Detección y Contención de Ransomware

Escenario

Un empleado ejecuta un archivo adjunto de correo electrónico que contiene un dropper de ransomware. El malware inicia procesos de reconocimiento, desactiva servicios de backup y comienza el cifrado de archivos.

Detección CTH

Indicador	Motor de Detección	Acción
PowerShell ofuscado ejecutándose	Correlación + EDR	Alerta HIGH generada
Conexión a dominio DGA (algorítmico)	Threat Intelligence + ML	Alerta CRITICAL
Intento de detener Volume Shadow Copy	Correlación SIGMA	Escalación automática
Cifrado masivo de archivos	UEBA (comportamiento anómalo)	Trigger de playbook

Respuesta Automatizada

1. Aislamiento: El endpoint infectado es aislado de la red en menos de 30 segundos.

2. Bloqueo C2: Las IPs y dominios de C2 se bloquean en el firewall perimetral.

3. Snapshot: Se dispara snapshot de sistemas críticos para recuperación.

4. Notificación: Equipo de respuesta notificado con análisis inicial completo.

Resultado

Contención en menos de 5 minutos. Impacto limitado a un endpoint. Sin pérdida de datos gracias a snapshots. Investigación forense completada en 4 horas con identificación de vector inicial.

6.2 Detección de Phishing Dirigido

Escenario

Una campaña de spear-phishing dirigida a ejecutivos de la organización utiliza dominios lookalike para robar credenciales corporativas.

Detección CTH

Threat Intelligence: Dominio identificado como lookalike registrado hace 48 horas.

Correlación: Múltiples usuarios accediendo al mismo dominio sospechoso.

UEBA: Patrones de login anómalos desde ubicaciones inusuales post-visita.

Respuesta

Bloqueo del dominio malicioso, reset forzado de credenciales de usuarios afectados, análisis de cuentas comprometidas, notificación a usuarios con capacitación adicional.

6.3 Detección de Acceso No Autorizado

Escenario

Un atacante utiliza credenciales robadas de una brecha de terceros para intentar acceder a sistemas corporativos.

Detección CTH

UEBA: Login desde ubicación geográfica nunca antes vista para el usuario.

Correlación: Múltiples intentos fallidos seguidos de acceso exitoso.

Threat Intelligence: IP de origen asociada a VPN comercial usada por actores maliciosos.

Respuesta

Sesión terminada inmediatamente, cuenta bloqueada, alerta a usuario legítimo, análisis de actividad durante el acceso, reset de credenciales y habilitación de MFA.

6.4 Amenaza Interna (Insider Threat)

Escenario
Un empleado con acceso privilegiado descarga grandes volúmenes de información confidencial antes de su renuncia planificada.

Detección CTH

UEBA: Volumen de descargas 500% superior al baseline del usuario.

DLP Integration: Detección de archivos clasificados siendo copiados a USB.

Correlación: Acceso a sistemas fuera de horario laboral habitual.

Respuesta

Alerta silenciosa a equipo de seguridad (sin notificar al empleado), documentación forense completa, coordinación con RRHH y Legal, preservación de evidencia para posibles acciones legales.

Resumen de Especificaciones

Categoría	Especificación
Producto	Cyber Threat Hunter (CTH) v0.02
Tipo	Managed Detection and Response (MDR) / SIEM
Fabricante	Postech
Despliegue	On-Premise, Nube Privada, Híbrido
Monitoreo	24/7/365 por Teliko SOC
IOCs Activos	209,565+
Fuentes de TI	12+ (OTX, CISA, SANS, Talos, etc.)
Detección	Correlación, UEBA, ML, Threat Intelligence, Firmas
Requisitos Mínimos	8 cores, 32 GB RAM, 500 GB SSD
SO Servidor	Ubuntu 22.04/24.04 LTS
Integraciones	EDR, Firewalls, SIEM, Cloud, ITSM
Cifrado	TLS 1.2+, AES-256
Autenticación	RBAC, MFA, SSO (SAML/OAuth/LDAP)
Frameworks	ISO 27001, NIST CSF, MITRE ATT&CK, PCI-DSS
SLA Disponibilidad	99.9%
SLA Compliance	> 99%
Soporte	24/7 (P1/P2), Email, Teléfono, WhatsApp
Licenciamiento	Por activos, volumen, usuarios o Enterprise