www.tssc.mx

Folleto

<CTH/>

CYBER THREAT HUNTER

Plataforma de Managed Detection and Response (MDR) desarrollada por **Tecnología y Servicios de Seguridad Cibernética S.A. de C.V. (TSSC)**.

Solución unificada que combina capacidades de **SIEM, SOAR, Threat Intelligence y User Behavior Analytics** para la detección, análisis y respuesta a amenazas cibernéticas en tiempo real.

Versión:0.02

¿POR QUÉ CTH?

¿Por qué implementar CTH en su organización?

El panorama de **amenazas cibernéticas** evoluciona constantemente, enfrentando a las organizaciones a ataques cada vez más sofisticados como **ransomware, amenazas persistentes avanzadas (APT), explotación de vulnerabilidades y amenazas internas.**

CTH fue **diseñado para atender estos desafíos mediante una plataforma unificada** que integra múltiples fuentes de datos y automatiza la respuesta a incidentes.

CTH ayuda a resolver:

Sobrecarga de alertas y falsos positivos

Reducción de falsos positivos mediante triaje automatizado y correlación inteligente.

Falta de visibilidad unificada

Consolidación de datos de múltiples herramientas en una sola vista integral.

Herramientas de seguridad en silos

Integración abierta con EDR, firewalls, SIEM, cloud e ITSM en una plataforma unificada.

Tiempos de respuesta elevados ante incidentes

Contención automatizada de amenazas en minutos en lugar de horas.

Escasez de talento especializado

Acceso a analistas expertos 24/7 sin necesidad de construir un SOC interno.

PROPUESTA DE VALOR:

CTH ofrece una propuesta de valor diferenciada como solución MDR para empresas y organizaciones:

Detección Avanzada de Amenazas

Utiliza múltiples motores de análisis: correlación de eventos, UEBA,machine learning y threat intelligence para identificar amenazas sofisticadas que evaden defensas tradicionales.

Respuesta Automatizada

Implementa playbooks que permiten contener amenazas en segundos,reduciendo el tiempo de respuesta (MTTR) y minimizando el impactode incidentes.

Visibilidad Unificada

Consolida información de múltiples fuentes de seguridad en dashboardsejecutivos y operacionales.

Cumplimiento Normativo

Facilita el cumplimiento de marcos regulatorios como ISO 27001,NIST CSF y MITRE ATT&CK mediante reportes automatizados.

Operación 24/7

Monitoreo continúo respaldado por el equipo de analistas

Beneficios Clave:

- Contención automatizada de amenazas en menos de **5 minutos**
- **Reducción del 80%** en el tiempo de investigación inicial
- Cumplimiento de **SLA superior al 99%**
- Reducción significativa del costo total de operación del SOC

Arquitectura General

CTH se despliega como solución:

- On-Premise
- Nube Privada
- Híbrido

MÓDULOS PRINCIPALES Y CIERRE

Dashboard
Visualizaciones ejecutivas y operacionales del estado de seguridad.

Resources
Gestión de activos y fuentes de datos integradas.

Threat Intelligence
Centro de inteligencia de amenazas con advisories e IOCs activos.

Threat Hunting
Búsqueda proactiva de amenazas y gestión de vulnerabilidades.

Helpdesk
Gestión del ciclo de vida de incidentes: investigaciones, tickets y métricas SLA.

Settings
Configuración de SLAs, usuarios y perfiles.

<CTH/>

CYBER THREAT HUNTER

GRACIAS

ventas@tssc.mx