

SH13LD-4CE



# SHIELD FORCE CSOC

CYSIV

Servicios Administrados de Ciber Seguridad

Virtual CSOC

## Beneficios

- Detección de Amenazas y Remediación
- Reducción de Costos
- Mejora la visibilidad, reporte y cumplimiento

“Cuanto más rápido se pueda identificar y contener una violación de datos, menores serán los costos. Las infracciones con un ciclo de vida de menos de 200 días fueron en promedio \$ 1.22 millones menos costosas que las infracciones con un ciclo de vida de más de 200 días”

- Ponemon Institute, 2019

## CSOC como Servicio

Combina todos los elementos de un servicio proactivo de caza de amenazas de un Centro de Operaciones de Ciber Seguridad (CSOC), con servicios administrados con cobertura sin interrupción 24 x 7, y un esquema de pago mensual basado en demanda y consumo. Nuestro CSOC opera como una extensión de su equipo de Ciber Seguridad incrementando y extendiendo sus capacidades.

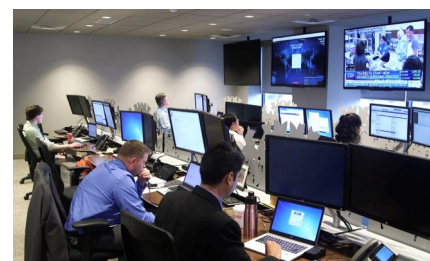


## CSOC Como servicio provee:

- Monitoreo de eventos de Seguridad, detección, investigación y alertamiento
- Caza de Amenazas proactivas, mapeo de incidentes en “Kill Chain” y al Framework ATT&CK de MITRE
- Gestión de Respuesta a Incidentes, incluyendo análisis de malware y análisis forense
- Gestión de Inteligencia de Amenazas (Colección, Fusión y Diseminación)
- Gestión de Vulnerabilidades y Amenazas
- Implementación, Gestión y Monitoreo de Productos de Seguridad
- Niveles de Servicio, RunBooks y Playbooks

## CSOC VIRTUAL

Nuestro CSOC Virtual en el modelo como servicio, aumenta las capacidades de las empresas que no cuentan con personal o con recursos suficientes de seguridad de la información para soportar sus operaciones e infraestructura



## Defensa Proactiva contra Amenazas



Nuestros expertos en conjunto con **Cysiv** monitorean su entorno en busca de amenazas, los investigan y evalúan, y realizan una caza de amenazas proactiva. Después, se realizan recomendaciones apropiadas, para que se tomen las acciones necesarias para remediarlas.

**NEXT-GEN SIEM:** **Cysiv** ha desarrollado su propio SIEM avanzado. Esta plataforma única y poderosa, nativa en la nube, co-administrada y multi-cliente combina una serie de tecnologías y funciones esenciales, aprovechando una amplia gama de técnicas avanzadas de ciencia de datos para automatizar, acelerar y mejorar el proceso de encontrar y priorizar amenazas que ameritan la investigación de una persona. Además, está respaldado por un “data lake” indexado, construido a la medida, masivamente escalable y con almacenamiento de datos por niveles (hot, warm y cold) para administrar mejor los costos y respaldar los requisitos de cumplimiento.

**Telemetría Empresarial:** Los registros, datos y otra telemetría de tantas fuentes relevantes como sea posible (controles de seguridad, infraestructura, incluida la nube (AWS®, Microsoft® Azure™, Google Cloud Platform™), aplicaciones y otras fuentes de datos contextuales, se normalizan primero para facilitar la correlación, reducir falsos positivos y ayudar a resaltar falsos negativos. Esto mejora la confianza en la detección para una mayor investigación. **Cysiv** es agnóstico al producto e ingiere telemetría de una gran cantidad de fuentes y fabricantes.

**Datos de Enriquecimiento:** la telemetría se enriquece con información sobre amenazas, incluida las evaluaciones de vulnerabilidad, inventarios de activos y Active Directory, para mejorar aún más la correlación, reducir los falsos positivos, ayudar a resaltar falsos negativos y para identificar actividad maliciosa.

**Expertos:** los expertos certificados de **SHIELDFORCE** y de **Cysiv**, incluidos analistas e ingenieros de seguridad, cazadores de amenazas e investigadores, científicos e ingenieros de datos y expertos en respuesta a incidentes, están directamente accesibles para usted. Los expertos operan como una extensión virtual para su equipo de seguridad, colaborando según sea necesario, para garantizar aún más la detección y protección oportuna.

## Servicios Administrados de Seguridad

Además, el CSOC administrará los dispositivos de seguridad que operen en su plataforma, de nube híbrida, seguridad de red y punto final. También integra controles de seguridad, monitorear su actividad, ajusta las reglas y políticas, implementa parches y actualizaciones, y realiza comprobaciones de estado periódicas para garantizar que se hayan optimizado para su entorno.

## Precio basado en Consumo

Activamos el servicio rápidamente, aseguramos que solo pague por los servicios y licencias que consume cada mes, a la vez que brinda la máxima flexibilidad y ahorro.

### 90 Días de Evaluación

- Definir Requerimientos Servicio
- Definir Escalamiento CSOC
- Integración e Ingestión
- Demostrar Valor

### Pagar bajo demanda

- Facturación Mensual por consumo
- Pago por uso, por unidad
- No Capex

### Contrato Firmado

- Facturación Mensual por Consumo
- Contrato Negociado
- Mínimo un año
- Descuento multianual

**SH13LD-4CE**

**SHIELD FORCE**  
www.shieldforce.mx

ventas@shieldforce.mx  
+52.55.53.51.15.56  
ext. 2010

**INCIDENT RESPONSE TEAM**  
S.A. DE C.V.  
Insurgentes Sur 1458 Piso 19,  
Col. Actipan, Alcaldía Benito Juárez,  
03230, Ciudad de México.