MISSION CRITICAL SOC

# OT EDR

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

## Telefónica Tech ofrece una solución para la protección de endpoints de entornos OT e IoT respaldados por la innovadora tecnología de TXOne Networks.

Estos servicios están diseñados para salvaguardar activos digitales frente a amenazas cibernéticas cada vez más sofisticadas. Proporcionan una solución integral de protección del endpoint que incluye inspección, auditoría, defensa desde la red y una gestión centralizada a través de consolas unificadas.

Debido al ritmo de cambio tecnológico y a la necesidad de contar con equipos especializados, la mayoría de las organizaciones no tienen la capacidad de responder a las sofisticadas amenazas actuales, lo que deriva en dolorosos procesos de negocio, grandes pagos de ransomware, gastos legales, pérdidas reputacionales, etc. La detección y respuesta efectiva requiere una tecnología de detección de primera clase, gestionada por un equipo humano especializado que permita evaluaciones proactivas de las amenazas y la rápida contención de los ataques.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

El servicio de protección de endpoints de Telefónica Tech está dirigido a una amplia gama de organizaciones industriales que operan en entornos OT como la industria manufacturera, energética, agroindustrial, química, minera, transporte, y un largo etc... Este servicio es crucial para aquellas empresas que enfrentan desafíos específicos relacionados con la convergencia de tecnologías IT (Tecnología de la Información), IoT (Internet of Things) y OT.

Nuestro servicio de seguridad profesional industrial va dirigido a aquellas organizaciones con la necesidad de abordar los siguientes desafíos de la industria:

**Mayor Conectividad y Superficie de Ataque:**
La integración de tecnologías IT y OT y el aumento de dispositivos conectados amplían las oportunidades para ataques cibernéticos.

**Sistemas Críticos y Sensibles:**
Los entornos industriales a menudo operan con sistemas que no pueden permitirse tiempo de inactividad, lo que hace que la seguridad y la resiliencia sean fundamentales.

**Amenazas Evolutivas:**
Las amenazas cibernéticas se están volviendo más sofisticadas, requiriendo soluciones avanzadas que puedan adaptarse y responder eficazmente.

**Visibilidad y Monitoreo:**
Muchas organizaciones carecen de visibilidad completa sobre sus sistemas OT, lo que dificulta la detección y respuesta a incidentes de seguridad.

**Regulaciones y Cumplimiento:**
Las industrias están sujetas a regulaciones estrictas que requieren la implementación de medidas de seguridad robustas para proteger datos e infraestructura crítica.

NUESTRA PROPUESTA DE VALOR

## Nuestro servicio

Telefónica Tech se centra en ofrecer una protección integral y avanzada para entornos industriales OT, con un enfoque en la Continuidad Operativa, implementando el modelo Zero Trust para asegurar cada componente y comunicación dentro del sistema, mitigando así los riesgos sin interferir con la operación continua. Proporcionando además un servicio de Implementación, soporte, mantenimiento y explotación de la tecnología.

## ¿Qué te permite?

**1. Soporte especializado:**

- Actualizaciones y mantenimiento.
- Recolección y análisis de logs.
- Gestión de políticas y perfiles.
- Monitorización y gestión de redes.

**2. Implementación:**

- Evaluación y planificación inicial.
- Adquisición de hardware y software.
- Configuración y preparación de dispositivos.
- Implementación y despliegue.

**3. Mucho más...**

- Detección y eliminación de malware en endpoints.
- Realización de inspecciones y auditorías de seguridad.
- Gestión centralizada de la seguridad a través de consolas.
- Innovación continua utilizando tecnología de vanguardia.
- Disponibilidad de un equipo experto con más de 15 años de experiencia en servicios de seguridad gestionada.
- Resiliencia y Redundancia, asegurando la alta disponibilidad y la segmentación segura de la red.
- Mejora de la visibilidad de sistemas OT, permitiendo una detección temprana y una respuesta rápida.

**4. Explotación de la tecnología:cializado:**:

- Monitoreo y generación de alertas.
- Actualización y mantenimiento proactivo.
- Generación de informes y análisis de datos.
- Representación gráfica y gestión de activos.

**5. Mantenimiento de los equipos:**:

- Evaluación inicial y diagnóstico.
- Gestión de los equipos.
- Monitoreo y gestión de contratos de mantenimiento.

## Beneficios del servicio

**1. Optimización del rendimiento y disponibilidad:**

La implementación, mantenimiento y actualización proactiva de hardware y software aseguran que los dispositivos funcionen de manera óptima, reduciendo tiempos de inactividad y mejorando la eficiencia operativa.

**2. Seguridad y cumplimiento:**

Los servicios de soporte especializado y explotación proactiva garantizan que los sistemas estén siempre protegidos contra nuevas amenazas, cumplan con las normativas de seguridad y mantengan la integridad de la información.

**3. Gestión eficiente de incidencias y actualizaciones:**

Con soporte reactivo y proactivo, así como mantenimiento continuo, se garantiza la rápida identificación y resolución de problemas técnicos, lo que minimiza interrupciones y maximiza la continuidad del negocio.

**4. Visibilidad y control mejorados:**

La recolección y análisis de logs, generación de informes y representaciones gráficas proporcionan una comprensión clara y detallada del estado de los sistemas, permitiendo a las organizaciones tomar decisiones informadas y estratégicas.

## Valor diferencial de Telefónica Tech

**Conocimiento experto de la tecnología:** Nuestro equipo está altamente capacitado y especializado en tecnologías EDR de vanguardia. No solo conocemos a fondo las herramientas más avanzadas del mercado, sino que también estamos en constante actualización para aplicar las mejores prácticas en la protección de tus sistemas frente a amenazas cibernéticas.

**Capacidades de implantación y explotación desde nuestro SOC:** Nuestros Centros de Operaciones de Seguridad (SOCs) son el corazón de la gestión del servicio. Desde aquí, realizamos una implantación eficiente de la solución EDR, asegurando su correcta configuración y un seguimiento continuo para detectar y responder a incidentes en tiempo real. Nuestra capacidad para monitorear, analizar y ajustar el sistema de manera proactiva garantiza que tu empresa esté siempre protegida.

**Experiencia en la gestión de servicios de seguridad para una amplia base de clientes:** Con años de experiencia en la gestión de servicios de ciberseguridad para un gran número de clientes, comprendemos la diversidad de necesidades en distintos sectores. Esto nos permite ofrecer un servicio flexible y adaptado, diseñado para maximizar la seguridad de acuerdo con las características particulares de cada negocio.

**Propuesta integral especializada en ciberseguridad industrial:** Nuestro enfoque de ciberseguridad va mucho más allá del EDR para entornos operativos (OT). Ofrecemos una solución integral que cubre todas las capas de seguridad en entornos industriales críticos, desde la protección de los sistemas de control hasta la monitorización de redes industriales, asegurando una defensa robusta y especializada para cualquier desafío.

## EQUIPO Y LOGROS

El equipo que respalda esta propuesta de ciberseguridad industrial está compuesto por especialistas en diversas áreas clave.

### 1. Operadores y Analistas de Ciberseguridad:

**Monitoreo y Respuesta:** Especialistas en la supervisión continua de endpoints para la detección y respuesta ante incidentes de seguridad, utilizando herramientas avanzadas de detección de malware y análisis de amenazas.

**Threat Intelligence:** Capacidad de alimentar sistemas de protección con inteligencia de amenazas en tiempo real para identificar y mitigar ataques emergentes.

### 2. Ingenieros de Seguridad y Consultores:

**Diseño e Implementación:** Responsables del diseño e implementación de soluciones de seguridad en endpoints, asegurando la protección contra malware y otras amenazas en dispositivos críticos.

**Evaluaciones y Auditorías:** Realizan evaluaciones de seguridad en endpoints para identificar vulnerabilidades y proponer mejoras en la postura de seguridad de la organización.

### 3. Especialistas en Tecnologías de Seguridad:

Implementación de soluciones de firewall de nueva generación (NGFW) para protección perimetral y segmentación de redes de producción.

Gestión centralizada de políticas de seguridad y acceso remoto seguro mediante ZTNA (Zero Trust Network Access.

Telefónica Tech ha logrado implementar y gestionar con éxito soluciones de ciberseguridad en diversos sectores industriales.
Algunos de los logros más destacados incluyen:

**1. Sector Energético:**

**Generación y Distribución de Energía:** Implementación de una solución de monitorización de seguridad OT que abarca múltiples ubicaciones, mejorando la visibilidad de los activos y la detección de vulnerabilidades.

**2. Sector Naval:**

**Construcción Naval Civil y Militar:** Diseño e integración de capacidades de ciberseguridad en plataformas navales de nueva generación, enfocándose en sistemas de control y combate.

**3. Sector Sanitario:**

**Líder en el Sector Sanitario Privado:** Visibilidad completa de activos de electromedicina, gestión de riesgos y personalización de soluciones de seguridad para integrarse con herramientas ya implantadas.

**4. Proyectos Internacionales:**

**Multinacionales en Diferentes Sectores:** Provisión de servicios gestionados de monitorización de seguridad para empresas en sectores como tratamiento de aguas, parques temáticos y logística, logrando una mejora significativa en la detección de amenazas y la protección de infraestructuras críticas.

## MODELO COMERCIAL

El modelo comercial de la propuesta se basa en una combinación de servicios gestionados y proyectos a medida, estructurados en varias fases:

**1. Evaluación Inicial:**
**Diagnóstico y Evaluación de Riesgos:** Realización de auditorías y evaluaciones de ciberseguridad para identificar activos críticos, vulnerabilidades y riesgos asociados.

**2. Planificación y Diseño:**
**Diseño de Arquitectura Segura:** Desarrollo de un plan detallado de arquitectura de red segura, incluyendo segregación y segmentación de redes, así como implementación de medidas de protección perimetral.

**3.Implementación:**
**Despliegue de Tecnologías:** Instalación y configuración de firewalls de próxima generación (NGFW), sistemas de autenticación y monitorización de seguridad para garantizar la protección continua de los entornos industriales.

**4.Gestión y Monitoreo Continuo:**
**Servicios Gestionados:** Provisión de servicios continuos de monitorización y gestión de seguridad, incluyendo análisis de tráfico, detección de amenazas y respuesta a incidentes mediante un Security Operations Center (SOC) especializado.

**5.Formación y Concienciación:**
**Capacitación:** Formación de personal interno en prácticas de ciberseguridad industrial, asegurando que los empleados sean capaces de identificar y responder adecuadamente a las amenazas.

**6.Optimización y Mejora Continua:**
**Revisión y Actualización:** Evaluación periódica de la postura de seguridad y actualización de las políticas y tecnologías implementadas para adaptarse a nuevos riesgos y desafíos.

PARTNERS RELACCIONADOS

txOne networks

SERVICIOS RELACCIONADOS

## OT & IoT Security Monitoring

Una solución integral para obtener visibilidad de los activos y detectar amenazas mediante el análisis del tráfico, ofrecida como servicio gestionado por Telefónica Tech como parte de un SOC especializado en entornos industriales y sanitarios.

## OT & IT segregation and OT segmentation

Una solución basada en el diseño e implementación de una arquitectura de red que permite segregar entornos IT y OT así como segmentar redes del entorno OT, complementada con tecnologías adicionales para avanzar en la aplicación de modelos ZeroTrust.

## Industrial Cyber Security Assessment

El servicio evalúa la ciberseguridad en entornos OT tomando como referencia la norma ISA/IEC 62443. Combina el análisis de la documentación aportada por la organización con una evaluación técnica basada en el análisis del tráfico de red capturado. Además, se puede llevar a cabo una evaluación de cumplimiento con respecto a las regulaciones aplicables, como ISA/IEC 62443 u otros estándares específicos de la industria (por ejemplo, NERC para energía, LPIC para infraestructura crítica). También incluye actividades de hacking ético para evaluar el nivel de seguridad de las infraestructuras.

Contáctanos para empezar la transformación digital de tu organización.