MISSION CRITICAL SOC

OT & IT Segregation and OT Segmentation

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Telefónica Tech ofrece este servicio especialmente diseñado para la industria que gestionan complejas redes de control.

Estas empresas suelen operar con múltiples plantas de fabricación, cada una con sistemas automatizados críticos, como líneas de montaje, robots industriales, sistemas SCADA (Supervisory Control and Data Acquisition), y otros dispositivos IoT y OT (Operational Technology).
El objetivo es garantizar que estas redes industriales estén protegidas frente a ciberataques, minimizando el riesgo de interrupciones en la producción que podrían tener un impacto significativo en la eficiencia operativa y la calidad del producto final.
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.

En los entornos industriales, suelen convivir aplicaciones y sistemas innovadores junto con equipos y sistemas de operación que llevan varios años en campo y que, muy probablemente, deban seguir en operación durante varios años más. Estos sistemas no siempre pueden actualizarse, por lo que es necesario, establecer mecanismos de protección que imposibiliten la explotación de las vulnerabilidades por parte de los cibercriminales. En este contexto, resulta imprescindible realizar e implantar un diseño seguro de la arquitectura de red basado en la segregación de los entornos IT y OT y la adecuada segregación de las redes OT.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

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

La propuesta de valor de **Telefónica Tech** en la segregación IT/OT y segmentación OT para la industria radica en la capacidad de ofrecer una **solución integral y personalizada** que asegura la integridad, disponibilidad, y confidencialidad de los sistemas industriales.

- **Diseño a medida:** Adaptación de la arquitectura de red a las necesidades específicas de la planta, teniendo en cuenta las particularidades de cada sistema de control y la naturaleza altamente automatizada de los procesos.
- **Tecnología avanzada:** Implementación de firewalls de nueva generación, sistemas de detección de intrusiones (IDS/IPS), y otras soluciones tecnológicas que aseguran que las redes OT estén completamente aisladas de las redes IT, evitando así que una brecha en la red corporativa afecte los sistemas de producción.
- **Cumplimiento regulatorio:** Asegurar que la empresa cumple con normativas de ciberseguridad industrial, como IEC 62443, y otros estándares aplicables, lo que no solo protege contra amenazas, sino que también facilita auditorías y revisiones regulatorias.

¿Qué te permite?

- **Aislar las redes OT críticas:** Garantizar que las redes que controlan los procesos de producción estén completamente separadas de las redes IT, reduciendo así la superficie de ataque y protegiendo los sistemas de control industrial (ICS) de posibles ciberataques.
- **Controlar y supervisar el tráfico de red:** Permitir una supervisión y control detallado del tráfico entre diferentes segmentos de la red OT, asegurando que solo las comunicaciones necesarias y autorizadas se realicen, limitando así los riesgos de movimientos laterales de amenazas dentro de la red.
- **Optimizar la seguridad y el rendimiento:** Mantener el equilibrio entre seguridad y eficiencia operativa, permitiendo que la planta continúe operando de manera fluida mientras se minimizan los riesgos de ciberseguridad.

Beneficios del servicio

1. Protección contra ciberataques avanzados:

Al segmentar la red OT, se reduce significativamente el riesgo de que un ciberataque comprometa sistemas críticos de producción. Esto es vital en un entorno donde la interrupción del proceso de producción puede llevar a pérdidas económicas significativas.

2. Mejora de la resiliencia operativa:

Con una red bien segmentada, un incidente en un segmento no afecta a toda la planta, lo que permite una rápida contención y recuperación, manteniendo la mayoría de las operaciones funcionando sin interrupciones.

3. Cumplimiento normativo:

Cumplir con las normativas de ciberseguridad específicas para el sector automotriz, lo que facilita las auditorías y mejora la confianza de los clientes y socios comerciales.

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

Experiencia y especialización: Telefónica Tech cuenta con un equipo de expertos en ciberseguridad industrial que entienden las necesidades específicas de cada sector. Esto incluye un conocimiento profundo de los sistemas de control industrial y los desafíos únicos que presentan.

Tecnología de vanguardia: Integración de tecnologías avanzadas, como firewalls de nueva generación y soluciones de monitoreo continuo, que están diseñadas para proteger entornos industriales altamente automatizados y garantizar la seguridad de los datos y la integridad de los procesos.

Enfoque integral y gestionado: Provisión de un servicio gestionado de extremo a extremo, que incluye desde la planificación y diseño de la arquitectura de red hasta la implementación y el monitoreo continuo, asegurando que la planta esté protegida en todo momento.

Escalabilidad y flexibilidad: Capacidad para adaptar y escalar la solución según las necesidades específicas de cada planta o línea de producción, asegurando que la ciberseguridad evolucione junto con la empresa.

Soporte continuo y local: Telefónica Tech ofrece soporte técnico especializado y local, asegurando que las soluciones de ciberseguridad se mantengan actualizadas y adaptadas a las últimas amenazas y necesidades del sector.

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

FORTINET paloalto NETWORKS CHECK POINT CISCO

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.

Aristeo

Red OT de captura y análisis predictivo de amenazas de Telefónica Tech que genera inteligencia con valor diferencial.

OT EDR

Protección integral y avanzada para entornos OT industriales, con énfasis en la continuidad operacional. Al implementar el modelo Zero Trust, protegen todos los componentes y comunicaciones dentro del sistema, mitigando así los riesgos sin interferir con las operaciones continuas. Además, ofrecen servicios de implementación, soporte, mantenimiento y gestión tecnológica. Un servicio 360º.

Contáctanos para empezar la transformación digital de tu organización.