MISSION CRITICAL SOC

OT&IoT Security Monitoring

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Te ayudamos a obtener visibilidad sobre los activos conectados a la red. Gestionamos las alertas relacionadas con las vulnerabilidades, amenazas de seguridad y anomalías que se produzcan en el entorno OT e IoT.

La tendencia actual es que las redes IT y OT/ IoT converjan, lo que plantea varios desafíos de seguridad. El primero de los retos es el de **tener visibilidad sobre los dispositivos conectados a la red y sus vulnerabilidades**, ya que lo que no se ve no se puede proteger. Un segundo reto es **identificar cualquier amenaza o anomalía** que pueda afectar al ecosistema y alertar sobre ello.

Para ello, en Telefónica Tech ofrecemos tecnologías especializadas en OT & IoT además de un equipo de expertos que operan el servicio desde nuestra red global de SOCs. Los analistas **alertan al cliente en tiempo real** sobre amenazas importantes y se pone a disposición del cliente una **serie de informes periódicos** para tener toda la información de lo que sucede en la red.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?

Empresas que hacen uso de tecnologías de operación (OT) e Internet de las cosas (IoT), como las de energía, fabricación, gestión del agua, alimentos y bebidas, química, farmacéutica, automatización de edificios, ferrocarriles, petróleo y gas, transporte, minería, sector automovilístico, etc.

Empresas que se quieran delegar la operación del servicio de monitorización, beneficiándose de la experiencia de los SOCs de Telefónica Tech y recibiendo avisos e informes sobre todo lo acontecido en su red.

Empresas y entidades públicas del sector médico y sanitario interesadas en **monitorizar la seguridad de sus entornos.**

NUESTRA PROPUESTA DE VALOR

Nuestro servicio

El servicio se opera desde nuestros SOCs, gestionando tanto las alertas referentes a la seguridad como a la salud de las sondas. Las alertas de seguridad pueden estar relacionadas con amenazas a los activos del cliente, anomalías en las variables del proceso o vulnerabilidades de los activos. Además, se muestran los activos conectados a la red, lo cual aporta gran visibilidad del entorno. El cliente recibe toda esta información de forma periódica en los informes que se le entregan además de avisos en tiempo real en caso de incidentes graves.

Adicionalmente, se ofrece el despliegue de las sondas en la infraestructura del cliente, las cuales analizan el tráfico de forma pasiva y son capaces de entender la mayoría de los protocolos industriales e IoT.

¿Qué te permite?

Este servicio te permitirá:

- **Tener visibilidad sobre los activos** conectados a la red monitorizada y sus vulnerabilidades.
- **Detectar las amenazas de seguridad** en el entorno, así como las anomalías que se produzcan tanto a nivel de seguridad como en relación con las variables del proceso.
- **Monitorizar la ciberseguridad de redes celulares privadas (4G y 5G)** mediante tecnologías específicas para estos entornos.
- **Contar con un equipo de expertos que gestionan las alertas y avisan en tiempo real de incidentes graves.**

Beneficios del servicio

Seguridad aplicada

El servicio identifica los activos conectados a las redes industriales y detecta amenazas de seguridad. Todo esto se realiza mediante análisis de una copia del tráfico, evitando perturbaciones en la red. Simplificamos significativamente el despliegue porque no depende de agentes que deban instalarse en los dispositivos.

Servicio gestionado

El cliente puede delegar la gestión del servicio, contando con la experiencia de nuestros expertos quienes operan el servicio 24x7. Se informa rápidamente ante incidentes graves y se envían reportes semanales con información sobre activos y amenazas, así como un informe de riesgos mensual.

Detección de ataques específicos del sector OT & IoT

La base de datos de amenazas se actualiza periódicamente con feeds industriales específicos. Además, las capacidades de detección incluyen anomalías en variables del proceso.

Capacidad de reacción

Informes enriquecidos y notificaciones en tiempo real para responder eficazmente a las amenazas cibernéticas.

Valor diferencial de Telefónica Tech

Integración con herramientas y flujos de trabajo de los SOCs optimizados mediante automatización, lo cual permite hacer un uso efectivo y eficiente de la tecnología, centrándose en los eventos más relevantes del cliente y agilizando su tratamiento.

Alertas e informes de seguridad con recomendaciones de remediación, lo que facilita la respuesta a incidentes y hace más eficaz la gestión de riesgos.

Escalabilidad global para proteger ubicaciones distribuidas, con expertos dedicados al servicio situados en diferentes geografías.

EQUIPO Y LOGROS

Nuestros equipos

- › **+100** millones de eventos de seguridad rastreados a nivel mundial cada año.
- **+1.800** empleados de SecOps.
- **+1.500** certificaciones de seguridad.
- **+12** tipos de certificaciones específicas del sector OT.

Logros

- Servicio **industrializado y replicable** en las diferentes geografías.
- Certificación **Nozomi MSSP Elite.**
- **+ 40** sondas en proyectos con clientes reales.

MODELO COMERCIAL

Tras un análisis de la red del cliente se establece el número de sondas a instalar en su infraestructura, el modelo y su ubicación. El servicio **incluye el hardware y software necesario, así como el despliegue y la configuración.**

Además, los expertos de la red global de SOCs de Telefónica Tech operan el servicio para que no tengas que preocuparte de nada, el cual se puede contratar con una **suscripción mensual.**

PARTNERS RELACIONADOS

NOZOMI NETWORKS

GARLAND TECHNOLOGY
See every bit, byte, and packet.®

SERVICIOS RELACIONADOS

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.

Cloud WiFi/SD-LAN

Optimiza el servicio con la conectividad integrada en tu sede, creando una solución SD-Branch regulada por las mismas políticas en toda la red y controlada desde un único dashboard que gestiona todas tus comunicaciones y seguridad.

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 Zero Trust.

Contáctanos para empezar la transformación digital de tu organización.

2025 © Telefónica Cybersecurity & Cloud Tech S.L.U. junto a Telefónica IoT & Big Data Tech S.A. Todos los derechos reservados.