Ciberseguridad & NaaS

Telefónica Tech

MISSION CRITICAL SOC

Te acompañamos en el viaje a la resiliencia de tu negocio

telefonicatech.com

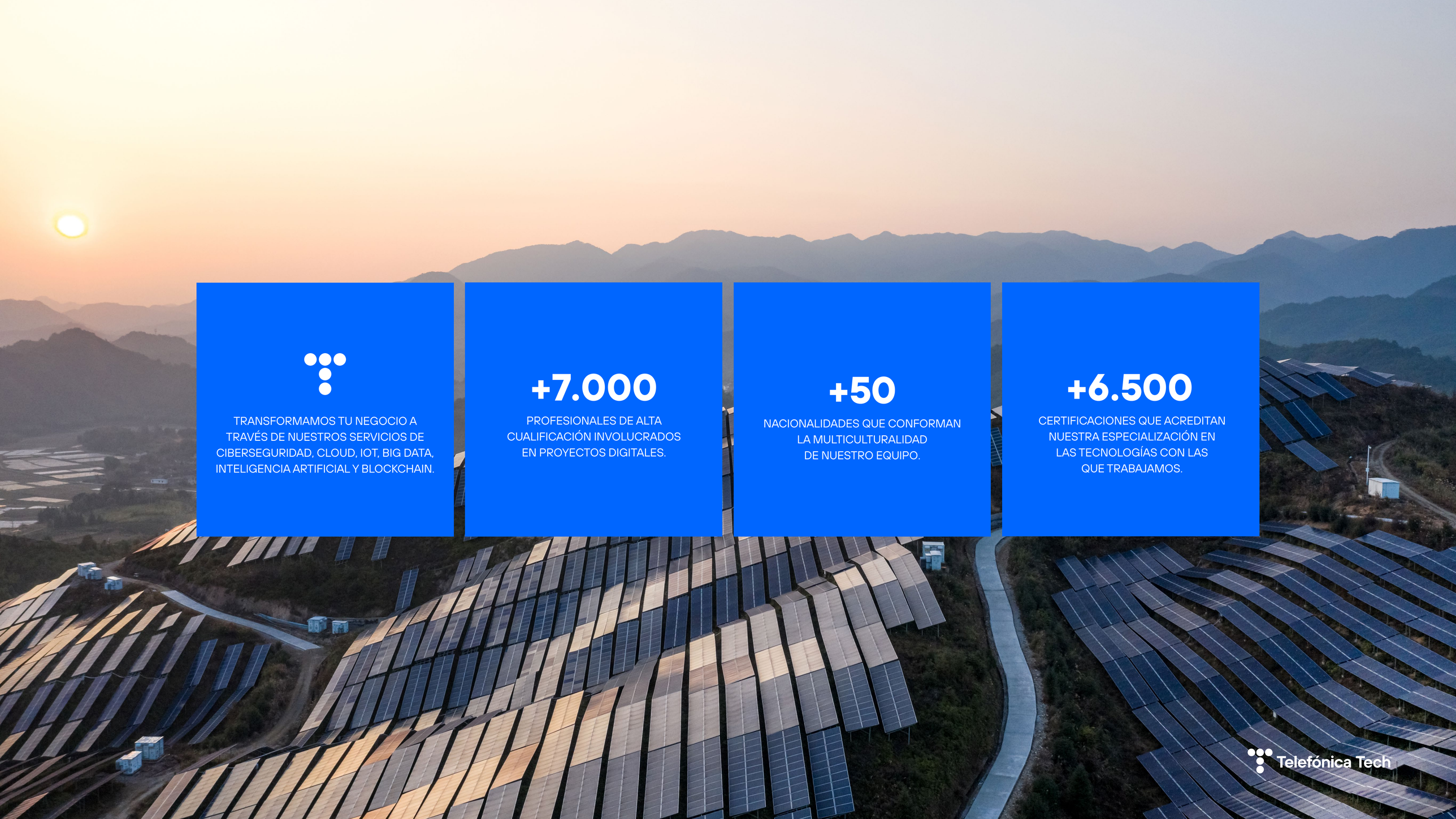
Telefónica Tech

El **SOC de Misión Crítica** de Telefónica Tech

La propuesta de **Mission Critical SOC** de Telefónica Tech está diseñada para proteger entornos críticos mediante la integración de tecnologías OT e IoT y un enfoque extremo a extremo que abarca personas, procesos y herramientas.

Actúa como un centro de operaciones (SOC) especializado para monitorizar, detectar, analizar y responder a ciberamenazas en sistemas ciberfísicos e infraestructuras críticas. Además, refuerza la ciberresiliencia con una fórmula basada en conocer el riesgo, proteger activos y establecer capacidades de detección, respuesta y recuperación.

TELEFONICATECH.COM



TRANSFORMAMOS TU NEGOCIO A TRAVÉS DE NUESTROS SERVICIOS DE CIBERSEGURIDAD, CLOUD, IOT, BIG DATA, INTELIGENCIA ARTIFICIAL Y BLOCKCHAIN.

+7.000

PROFESIONALES DE ALTA CUALIFICACIÓN INVOLUCRADOS EN PROYECTOS DIGITALES.

+50

NACIONALIDADES QUE CONFORMAN LA MULTICULTURALIDAD DE NUESTRO EQUIPO.

+6.500

CERTIFICACIONES QUE ACREDITAN NUESTRA ESPECIALIZACIÓN EN LAS TECNOLOGÍAS CON LAS QUE TRABAJAMOS.

Telefónica Tech

¿Quién es Telefónica Tech en Mission Critical SOC?

Ofrecemos una propuesta de ciberseguridad gestionada, diseñada para proteger infraestructuras críticas y entornos ciberfísicos, que integra monitorización 24/7, detección avanzada, respuesta ante incidentes y cumplimiento normativo OT/IoT.

+30

PROFESIONALES

DEDICADOS EXCLUSIVAMENTE A CIBERSEGURIDAD OT & IOT

1

DOC

CON DOS UBICACIONES GEOGRÁFICAS CON PROFESIONAES ESPECIALIZADOS EN OPERACIONES DE CIBERSEGURIDAD OT

+15

SECTORES

DESDE ENERGÍA, HIDROCARBUROS Y PAPEL, HASTA HOSPITALES, PUERTOS Y PARQUES TEMÁTICOS

+80

CERTIFICACIONES EN CIBERSEGURIDAD OT

COMO POR EJEMPLO: IEC 62443, FORTINET NSE OT, TXONE, CISCO, CLAROTY, ENTRE OTRAS

- **+100k** DISPOSITIVOS DE OT MONITORIZADOS
- **+10** OFICINAS TÉCNICAS ACTIVAS
- **+340** DISPOSITIVOS DE MONITOREO OT IMLEMENTADOS EL ÚLTIMO AÑO
- **3** PLATAFORMAS LÍDERES OT INTEGRADAS PARA VISIBILIDAD TOTAL Y DETECCIÓN
- **~60** EVALUACIONES DE SEGURIDAD INDUSTRIAL

Telefónica Tech

Un Digital Operations Center (DOC) con dos ubicaciones geográficas y una red global de SOCs

Desarrollando las mejores capacidades extremo a extremo de su clase en seguridad cibernética y operaciones en la nube.

- ALCANCE GLOBAL Y PRESENCIA LOCAL
- 24/7/365 PROFESIONALES DE SEGURIDAD SIEMPRE ACTIVOS
- EQUIPO MULTIDISCIPLINAR
- SINERGIAS PARA UNA MEJOR EXPERIENCIA DE CLIENTE
- LAS MEJORES PLATAFORMAS E INFRAESTRUCTURAS
- VISIÓN INTEGRADA CON UN ÚNICO PUNTO DE CONTACTO

Telefónica Tech

Ciberseguridad & NaaS

Mission Critical SOC

Aumentamos la resiliencia de tus infraestructuras críticas con ciberseguridad avanzada, ofrecemos soluciones personalizadas para detectar, responder y recuperar ante amenazas en entornos industriales OT e IoT.

Telefónica Tech

Industrial Cyber Security Assessment

DESCUBRE MÁS EN NUESTRA WEB

Evaluamos 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 se incluyen actividades de hacking ético para evaluar el nivel de seguridad de las infraestructuras.

SOBRE EL SERVICIO

El servicio permite evaluar el nivel de ciberseguridad de los entornos OT tomando como referencia principal la norma ISA/IEC 62443. Esta evaluación se realiza combinando el análisis de información y documentación proporcionada por la organización con una evaluación técnica que parte del análisis del tráfico de red capturado en estos entornos.

Adicionalmente, puede proporcionarse una evaluación de conformidad normativa con respecto a la mencionada ISA/IEC 62443 u otras que apliquen al sector en cuestión (e.g. NERC para el sector energético, LPIC en infraestructuras críticas). Asimismo, también se incluyen actividades de hacking ético que permitan evaluar el nivel de seguridad de las infraestructuras.

¿QUÉ PERMITE?

- Tener visibilidad de los entornos operacionales (activos, arquitectura de comunicaciones) y conocimiento de su nivel de seguridad.
- Disponer de una propuesta de arquitectura y soluciones de seguridad.
- Definir un plan director de ciberseguridad industrial con el que establecer una hoja de ruta para la implementación de soluciones.

BENEFICIOS

Informe de la actividad

Nuestro equipo se encarga de la elaboración y presentación de un informe que resume las actividades realizadas, los hallazgos en materia de ciberseguridad y las recomendaciones de mejora.

Propuesta de soluciones recomendadas

El catálogo de productos y servicios existentes complementan la solución ofreciendo propuestas concretas para implementar las acciones identificadas en el plan director.

Plan director de seguridad

Como complemento al informe, es posible extender la actividad mediante la elaboración de un plan director de seguridad que permita trazar una hoja de ruta en la implementación de soluciones de ciberseguridad y alcanzar los niveles de seguridad establecidos definiendo hitos que ayuden a controlar el progreso.

OT & IT Segregation & Segmentation

DESCUBRE MÁS EN NUESTRA WEB

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.

SOBRE EL 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.

¿QUÉ 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

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.

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.

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.

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.

OT & IoT Security Monitoring

DESCUBRE MÁS EN NUESTRA WEB

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.

SOBRE EL SERVICIO

El servicio se opera desde nuestro DOC y 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.

¿QUÉ PERMITE?

- Tener visibilidad sobre los activos conectados a la red monitorizada y sus vulnerabilidades.
- Enriquecimiento del inventario de activos mediante el etiquetado automático de activos y alertas para mejorar la gestión de riesgos con herramienta propia (Telefónica Custom Tag*).
- 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

Visibilidad y mitigación de riesgos con un impacto mínimo en la red

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.

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.

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.

OT EDR

DESCUBRE MÁS EN NUESTRA WEB

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 360°.

SOBRE EL SERVICIO

Telefónica Tech se centra en ofrecer una protección integral y avanzada para entornos industriales OT, con un enfoque en la Continuidad Operativa, con un modelo robusto asegurando 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 PERMITE?

Permite a las empresas industriales garantizar la continuidad operativa al ofrecer una protección integral y avanzada para sus entornos de Tecnología Operativa (OT), asegurando cada componente y comunicación del sistema, lo que ayuda a mitigar riesgos sin interrumpir las operaciones. Además, proporcionamos servicios de implementación, soporte, mantenimiento y operación de la tecnología, asegurando una gestión eficiente y segura de sus sistemas.

BENEFICIOS

Optimización del rendimiento y disponibilidad

La gestión proactiva de hardware y software asegura un funcionamiento óptimo, minimizando el tiempo de inactividad y mejorando la eficiencia operativa.

Gestión eficiente de incidencias y actualizaciones

El soporte reactivo y proactivo, junto con el mantenimiento continuo, garantiza una rápida resolución de problemas, reduciendo interrupciones y asegurando la continuidad del negocio.

Seguridad y cumplimiento

El soporte especializado y la explotación proactiva protegen los sistemas contra amenazas, asegurando el cumplimiento de normativas de seguridad y la integridad de la información.

Visibilidad y control mejorados

El análisis de logs, informes y gráficas ofrece una visión clara del estado de los sistemas, permitiendo tomar decisiones informadas y estratégicas.

Aristeo – Deception as a Service

DESCUBRE MÁS EN NUESTRA WEB

Los sistemas de engaño (Deception Technology) mejoran sustancialmente los mecanismos de detección mediante la detección temprana de actividad maliciosa y el mejor conocimiento de los cibercriminales.

SOBRE EL SERVICIO

Nuestra plataforma DaaS integra dos tipos de soluciones: una es la plataforma Aristeo de ciberinteligencia avanzada (patentada y desarrollada íntegramente desde el área de Innovación de Telefónica TECH) que emplea hardware industrial real, la segunda son sistemas y appliances de terceros líderes en el mercado en el desarrollo de casos de engaño.

La integración de las dos tecnologías asegura la autenticidad y precisión de la información sobre amenazas. Ofrecer una solución conjunta, innovadora y diferencial, diseñada para adaptarse a las necesidades específicas de cada cliente, permitiendo la configuración de los señuelos para representar cualquier proceso industrial o sector productivo.

¿QUÉ PERMITE?

- **Captura y análisis predictivo:** Creación de señuelos industriales atraen atacantes para analizar sus tácticas y prever amenaza
- **Simulación realista:** Interacción con señuelos reales para captar mejor el comportamiento de amenazas.
- **Inteligencia predictiva:** Detección patrones para anticipar ataques y proteger activos críticos.
- **Integración con defensa existente:** Funciona con SIEM y TIP gestionados por SOC propios o del cliente.
- **Continuidad operativa:** Operativa sin alterar la infraestructura ni interrumpir operaciones.
- **Informes personalizados:** Generación análisis detallados para mejorar la seguridad según necesidades.

BENEFICIOS

Detección avanzada de amenazas

Identificación temprana de amenazas avanzadas, incluyendo grupos APT (Advanced Persistent Threats) y vulnerabilidades desconocidas (0-day).

Inteligencia predictiva

Análisis continuo de las amenazas para prever posibles ataques y reforzar la seguridad.

Adaptabilidad y flexibilidad

Capacidad para adaptarse a las infraestructuras y procesos específicos del cliente, sin necesidad de ocupar espacio en su infraestructura ni en sus instalaciones en el caso de señuelos físicos, aunque el servicio también está disponible on premise.

Protección constante

Nuestra solución DaaS opera 24x7, proporcionando vigilancia continua y actualizaciones en tiempo real sobre nuevas amenazas.

Compatibilidad con el cumplimiento normativo

DaaS facilita el cumplimiento de normativas y estándares de ciberseguridad del sector, ofreciendo un entorno de pruebas para verificar la adecuación de las medidas de protección contra amenazas actuales y emergentes.

Telefónica Tech

¿Listo para transformar tu empresa?

Telefónica Tech es la compañía líder en trasformación digital. Cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Business Apps, Ciberseguridad y NaaS, Cloud Híbrida, Conectividad e IoT, IA & Data, Future Workplace y Consultoría y Servicios Profesionales.

telefonicatech.com