

CONTINUOUS THREAT EXPOSURE MANAGEMENT

# Tactical Intelligence

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Refuerza tu detección y respuesta ante amenazas emergentes con inteligencia táctica accionable.

En un entorno donde las amenazas evolucionan constantemente y muchas logran evadir las defensas tradicionales, contar con inteligencia de amenazas integrada en tus dispositivos de seguridad marca la diferencia. Mejora la detección, agiliza la investigación y automatiza la respuesta ante incidentes.

Gracias a nuestra plataforma **NextDefense** y a un ecosistema de más de 160 fuentes internas, privadas y públicas, el servicio **Tactical Intelligence** te proporciona un feed curado, accionable y actualizado de indicadores de compromiso (IoC).

Este feed se integra directamente en tu infraestructura de seguridad para ampliar la visibilidad y acelerar la toma de decisiones.

De esta manera, ayudamos a tu organización a reducir el tiempo de exposición, priorizar lo realmente crítico y responder con mayor eficacia frente a las amenazas.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?



Empresas que buscan adoptar una postura proactiva en la detección y respuesta mediante inteligencia táctica integrada en sus SIEM, EDR, IPS, SOAR u otros controles.



Organizaciones que desean aprovechar inteligencia verificada, en tiempo real, sin depender solo de fuentes *open source*.



Clientes que no disponen de tiempo o recursos para construir, validar o mantener un *feed* propio de IoC.



Equipos de seguridad que quieran ahorrar tiempo en el proceso de investigación, reduciendo falsos positivos.

## Nuestro servicio

Tactical Intelligence es un servicio gestionado que proporciona acceso a feeds de inteligencia táctica con indicadores de compromiso (IP, dominios, URL, hashes) clasificados y enriquecidos. Estos indicadores se generan a partir de más de 160 fuentes públicas, privadas y propias, incluyendo la actividad observada en los servicios gestionados por Telefónica Tech, investigaciones internas y alianzas como la Cyber Threat Alliance o el programa AEGIS de Cisco.

El *feed* puede entregarse en formato STIX/TAXII, CSV o texto, y está disponible en dos modalidades (Lite y Full), adaptándose a tus necesidades y madurez. La integración puede ser autogestionada o realizada por Telefónica como parte de un servicio más amplio. Además, puedes ampliar el servicio con un *add-on* que permite la subida de tus propios indicadores para centralizar la entrega de todas tus fuentes de inteligencia en un solo punto.

## ¿Qué te permite?

- Recibir un feed curado de IoC, alineado con criterios de riesgo y confianza.
- Integrar estos indicadores en tus sistemas de seguridad para una detección más rápida y eficaz.
- Reducir el tiempo medio de detección (MTTD) y de respuesta (MTTR) ante incidentes.
- Ampliar la visibilidad sobre amenazas activas, con contexto enriquecido (tipo de amenaza, sector, región, CVE, TTP. etc.).
- Personalizar la ingesta, la política de caducidad, los umbrales de riesgo y confianza, para tener un *feed* a tu medida.
- Aprovechar la inteligencia generada por los servicios globales de Telefónica Tech.

## Beneficios del servicio

### Prevención

Permite reforzar tu perímetro de seguridad y los sistemas internos mediante el uso de inteligencia procesable, bloqueando amenazas antes de que se materialicen.

### Respuesta automatizada

Activa mecanismos de respuesta automática ante amenazas conocidas.

### Detección proactiva

Mejora la capacidad de detección temprana de amenazas de tu stack de seguridad mediante la correlación directa con IoC frescos y relevantes.

### Adaptabilidad

Ajusta el servicio acorde con tus necesidades, con opciones de personalización y gestión flexible.

## Valor diferencial de Telefónica Tech



Como MSSP, somos generadores de nuestra propia inteligencia de amenazas, que combinamos con una amplia variedad de fuentes de nuestro ecosistema de partners y alianzas estratégicas.



Participamos activamente en alianzas estratégicas como la Cyber Threat Alliance y la Red Nacional de SOC española.



Adaptamos nuestro servicio para satisfacer las necesidades y perfiles de riesgo de cada cliente, ofreciendo un enfoque personalizado.

### EQUIPO Y LOGROS

#### Nuestros equipos

- Unidad dedicada de analistas de inteligencia que presta servicio a nivel mundial desde los Centros de Operaciones Digitales (DOC), ubicados en España y Colombia.
- +29M de indicadores de compromiso en nuestra plataforma de inteligencia.
- Amplia experiencia en integraciones con tecnologías como SIEM, TIP, SOAR, EDR...

#### Logros

- Reconocidos por el CCN-CERT como principal contribuidor en inteligencia de amenazas a la Red Nacional de SOC española por dos años consecutivos.
- Colaboración constante con alianzas globales y organismos de referencia en la compartición de inteligencia sobre amenazas emergentes.

### PARTNERS RELACIONADOS



## MODELO COMERCIAL

Tactical Intelligence es un servicio con una cuota de suscripción recurrente, disponible en modalidad Lite o Full, con una amplia variedad de opciones de personalización y gestión adaptadas a cada cliente (integración gestionada por otros servicios o por el propio cliente, entrega vía TAXII o URL, umbrales de riesgo y confianza, tipos de indicadores a recibir, fuentes a consumir, política de caducidad, número de feeds a crear, posibilidad de añadir indicadores propios de cliente para su uso exclusivo).

No requiere despliegues complejos y puede integrarse fácilmente en los sistemas existentes.

## NUESTRAS SOLUCIONES

### Descubre todas nuestras soluciones

Creemos en el poder transformador de la tecnología para mejorar procesos, optimizar recursos y abrir nuevas oportunidades de negocio.



Contáctanos para empezar la transformación digital de tu organización.

