

CONTINUOUS THREAT EXPOSURE MANAGEMENT

# Red Team Assessment

¿CÓMO TE AYUDAMOS DESDE TELEFÓNICA TECH?

Las amenazas reales no tienen restricciones de tiempo y alcance. Nuestro servicio Red Team te permite medir tus defensas ante tus adversarios.

Comúnmente confundido con Penetration Testing, las cuales son pruebas definidas, de alcance limitado y puntuales que tienen objetivos específicos para su éxito o fracaso. Por el contrario, **un Red Team corporativo es un servicio continuo que se ejecuta durante largos periodos**, se realiza desde una perspectiva lo más cercana posible al conocimiento cero, de alcance no limitado y cuyo objetivo principal es mejorar las defensas ya existentes, es decir, el Blue Team.

**Nuestro servicio Red Team de Telefónica Tech está diseñado para probar y mejorar continuamente la eficacia y la capacidad de detección y respuesta de las defensas de seguridad de la información de las empresas** simulando escenarios de ataque mediante el uso de Técnicas, Tácticas y Procedimientos (TTPs) de los adversarios reales.

Proporcionamos a las empresas una **evaluación independiente con una inmersión profunda en los riesgos y vulnerabilidades** de la empresa y que sirve como referencia para medir las futuras mejoras en seguridad.

¿A QUIÉN VA DIRIGIDO ESTE SERVICIO?



Organizaciones de una alta madurez en seguridad y con equipos ya establecidos de **SecOps que buscan evaluar, medir y mejorar** sus capacidades de protección, detección y respuesta ante incidentes de seguridad de una forma continua y realista.



Empresas que buscan desarrollar a largo plazo capacidades sofisticadas propias de **Red Team Assessment** y optan por crecer y aprender de un partner de confianza.



Compañías pertenecientes al sector de infraestructuras críticas, sector público o que almacenen o procesen datos de carácter personal o información clasificada y se vean sujetas a **cumplimientos normativos**.

NUESTRA PROPUESTA DE VALOR

## Nuestro servicio

Realizamos simulaciones de ataques contra personas, software, hardware e infraestructuras, desde la perspectiva de los ciberdelincuentes, utilizando tácticas, técnicas y procedimientos observados en ataques recientes reales. De este modo, identificamos y explotamos las vulnerabilidades encontradas y demostramos cómo podrían dañar tus activos más críticos.

Cada uno de estos ataques se adapta a tu organización, considerando tanto los aspectos tecnológicos, como los de negocio. El servicio cuenta con un Red Team dedicado con conocimientos y habilidades multidisciplinares, cuya misión es diseñar y ejecutar los diferentes escenarios de ataque (ingeniería social, pruebas de intrusión física, pruebas de intrusión de aplicaciones, sistemas y comunicaciones), en base a la inteligencia de amenazas obtenida sobre los activos tecnológicos y/o humanos de tu organización.

## ¿Qué te permite?

Este servicio te permitirá:

- Disponer de evaluación exhaustiva e independiente de las **fortalezas y debilidades** de tu seguridad.
- Obtener una orientación clara y concisa sobre **cómo proteger tu información** ante sofisticados ataques de hoy en día.
- Ganar **experiencia persistente ante amenazas** de nueva generación y vulnerabilidades desconocidas sin riesgos reales

## Beneficios del servicio

### Comprueba el impacto real de un ataque dirigido

Sin sufrir las consecuencias reales de éste y justifica la asignación de recursos de seguridad y si se están utilizando eficazmente para mitigar y prevenir las amenazas.

### Un análisis completo de las fortalezas y debilidades de tu seguridad

Recibe la información esencial destilada que tu empresa necesita y transmítela de forma que sea valiosa tanto para los ejecutivos no técnicos como para el equipo técnico de seguridad.

### Gana experiencia persistente

Ante amenazas de nueva generación y vulnerabilidades desconocidas sin riesgos reales. Aumenta la concienciación, motivación y preparación de tu equipo de seguridad, ya que las defensas se prueban constantemente y se adaptan a la evolución continua del entorno.

## Valor diferencial de Telefónica Tech



Ejecutamos simulaciones de adversarios diseñadas para emular escenarios del mundo real, cubriendo vectores de ataque para entornos ciber, físico y humano.



Mantenemos contacto y comunicación cercanos con equipos internos de defensa y de respuesta ante incidentes con reuniones de seguimiento, presentaciones ejecutivas e informes técnicos con explicaciones detalladas.



Nuestra estructura Purple Teaming promueve una colaboración entre Red Team y Blue Team centrada en los intereses de la organización y sacando el máximo provecho de las simulaciones.

### EQUIPO Y LOGROS

#### Nuestros equipos

- **+2.200** empleados de SecOps.
- **+3.000** certificaciones de seguridad.
- **+100** pentesters a nivel mundial.
- **+50** analistas globales de seguridad.

#### Logros

- **+14000** horas realizando ejercicios Red Team en el último año.
- **98%** de nuestros clientes fueron comprometidos con éxito en los ejercicios Red Team.
- **90%** de los casos nuestro Red Team fue capaz de lograr el primer objetivo en los primeros 5 días.
- **85%** de los casos nuestro Red Team fue capaz de comprometer el primer activo en menos de 24 horas.
- **75%** de nuestros clientes creían que sus defensas de seguridad estaban preparadas ante cualquier amenaza.

### MODELO COMERCIAL

Nuestro servicio se ofrece en tres modalidades:

- Ejercicio completo de Red Team de **3 meses**, con reuniones de seguimiento e informes técnicos y ejecutivos.
- Ejercicios TIBER ES de **4 meses**, que te permite cumplir con la normativa TIBER del Banco de España.
- Servicio de Red Team de **12 meses** que añade una monitorización continua en busca de cambios en la infraestructura expuesta y el filtrado de información en internet.

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.

