twoko

Offensive Prevention

Creamos soluciones de ciberseguridad vanguardistas para protegerte de los problemas actuales.

Ciberseguridad, al siguiente nivel

Somos tu próximo socio estratégico

Robustecer la seguridad de las empresas, aportando un alto grado de predictibilidad y resiliencia en la operación TI, es clave, y eso lo sabemos en TWOKO. Es por eso que investigamos, identificamos y explotamos vulnerabilidades para estar mejor preparados a los ataques de cibercriminales. Nuestro objetivo es claro, ser un socio estratégico que garantice dos puntos importantes: Continuidad operacional y éxito en los negocios.

Entendemos que el panorama de la ciberseguridad es desafiante y en constante evolución. En base a esto, desarrollamos un conjunto completo de soluciones y servicios diseñados para proteger los activos digitales de nuestros clientes. Mediante la implementación de las últimas tecnologías y las mejores prácticas en ciberseguridad, minimizamos las vulnerabilidades y prevenimos incidentes que podrían afectar dos pilares del negocio: Reputación y operaciones.

Nuestro enfoque

Cercanía, profesionalismo y proactividad. Una mirada transversal para afrontar problemas del ahora.

Equipo multidisciplinario

Nuestro equipo de expertos altamente capacitados y experimentados en ciberseguridad trabaja de cerca con cada cliente para entender sus necesidades específicas y ofrecer soluciones personalizadas.

Enfoque integral

La implementación de soluciones de seguridad, monitoreo proactivo de amenazas, educación en ciberseguridad, y la respuesta rápida a incidentes son parte del enfoque 360 de Twoko.

Vanguardia

Mediante la implementación de las últimas tecnologías y las mejores prácticas en seguridad de la información, ayudamos a las empresas a minimizar las vulnerabilidades y a prevenir incidentes de seguridad.

Conoce nuestros servicios

La ciberseguridad requiere rigurosidad, experiencia y conocimiento. En Twoko diseñamos servicios para protegerte de las amenazas actuales con una mirada proactiva.

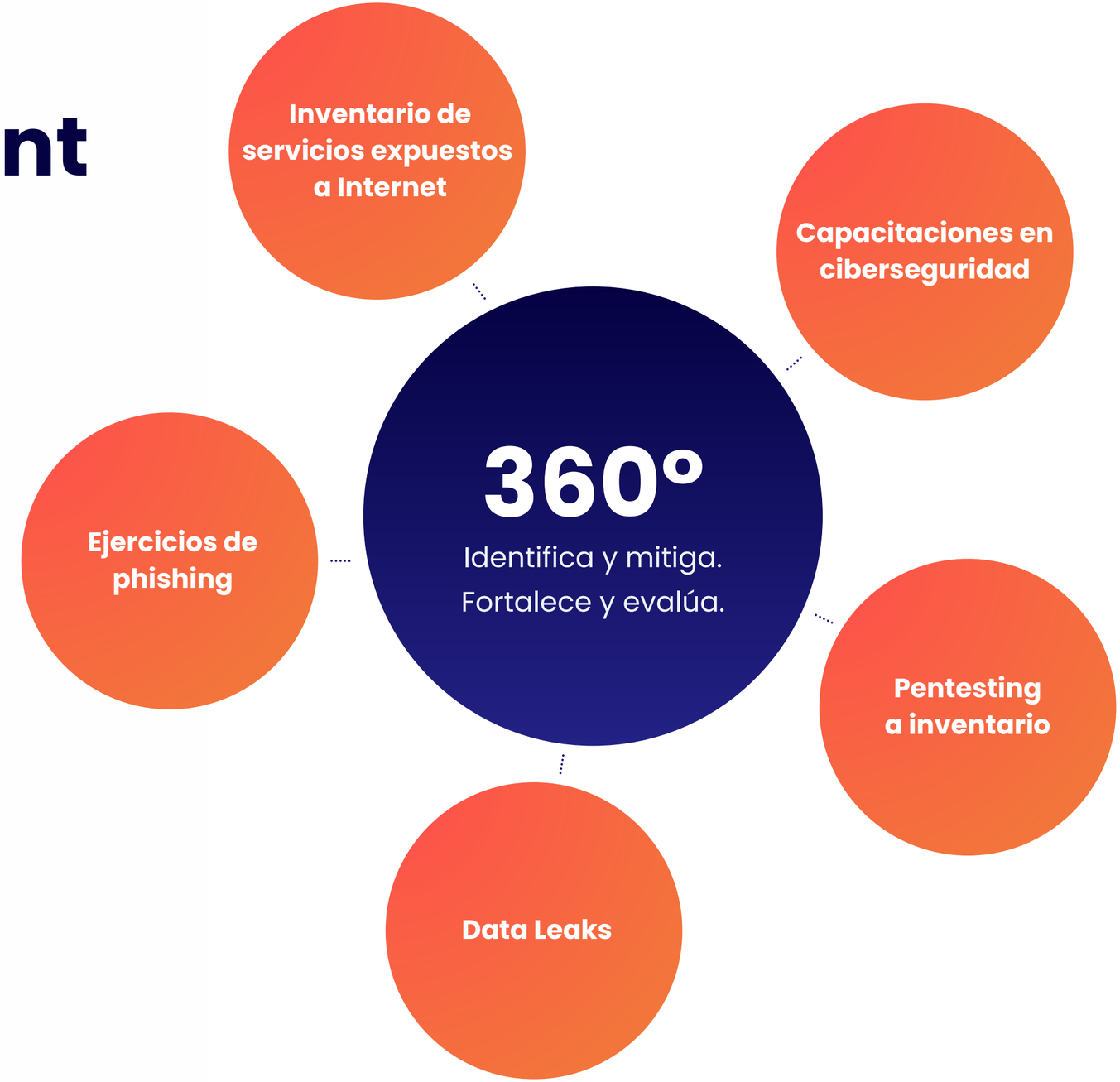
Te invitamos a descubrir más sobre:

1. Cyber Posturement
2. Cyber Intelligence I+D
3. Ethical Hacking
4. Ethical Phishing & Smishing
5. Análisis de vulnerabilidades
6. Red Team

1.

Cyber Posturement

Cyber Posturement es un servicio integral de seguridad diseñado para ofrecer una protección completa y proactiva a tu organización frente a las amenazas cibernéticas.



Inventario de servicios expuestos a Internet

Proporcionamos un inventario detallado de todos los servicios expuestos a Internet, incluyendo dominios, direcciones IP y otros componentes críticos.

Sabías que la gestión de activos es fundamental para un programa sólido de ciberseguridad.

Las brechas en el inventario, tanto para los activos locales como para los recursos de la nube, pueden dejar las superficies de ataque expuestas y ralentizar las capacidades de detección y respuesta.

Pentesting a inventario

Realizamos pruebas de penetración exhaustivas en el inventario identificado para descubrir y mitigar vulnerabilidades.

Sabías que nuestro servicio de Pentesting a inventario incluye:

- Infraestructura o Web: Evaluación de vulnerabilidades en hasta 3 direcciones IP o URL.
- Cloud: Evaluación de seguridad en entornos cloud, incluyendo hasta 3 API o URL.
- Aplicaciones Móviles: Pruebas de seguridad en una aplicación móvil.

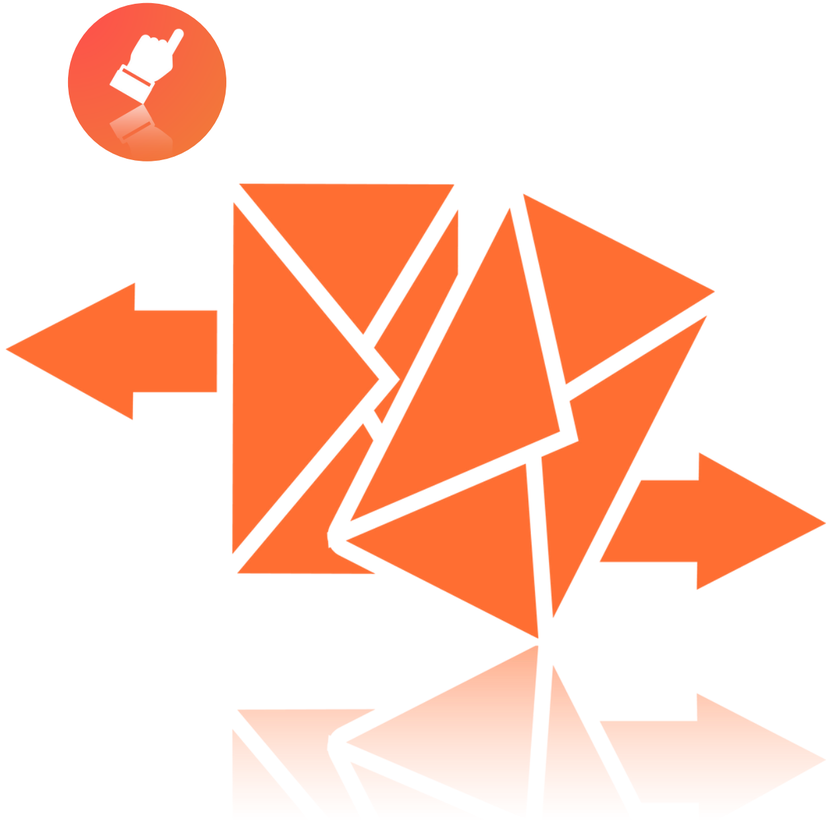
Ejercicios de phishing

Realizamos un ejercicio de phishing controlado para evaluar y mejorar la respuesta de tus empleados ante posibles ataques de ingeniería social.

Sabías que...

94% de las organizaciones a nivel global son víctimas de ataques de phishing.

60% menos de errores comenten las organizaciones que tienen un plan entrenamiento.

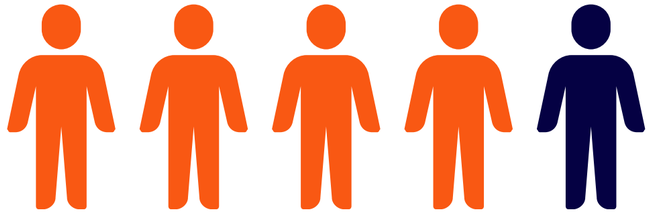


Data Leaks

Monitoreo y detección de filtraciones de datos en la web profunda y la dark web, para identificar y gestionar cualquier exposición de información sensible.

Sabías que el costo de una brecha de datos puede ascender a...

US $ 4.5M



15
Cuentas corporativas filtradas

Capacitaciones en Ciberseguridad

Ofrecemos seis sesiones de capacitación de dos horas cada una, enfocadas en la cultura de ciberseguridad y otros temas relevantes según las necesidades y el nivel de maduración de cultura de ciberseguridad de tu organización.

Sabías que las capacitaciones...

- Permiten abordar temáticas de manera directa, asegurando una interacción con el colaborador y que este entienda desde conceptos básicos hasta métodos para reportar correos maliciosos o posibles incidentes.

2.

Cyber Intelligence I+D

Investigación y desarrollo de soluciones avanzadas en ciberinteligencia. Un servicio que te entregará una ventaja proactiva en la identificación, análisis y mitigación de amenazas cibernéticas emergentes y sofisticadas.

Investigación avanzada

Nuestro equipo de expertos realiza investigaciones profundas sobre las últimas tendencias en amenazas cibernéticas, vulnerabilidades y tácticas utilizadas por actores malintencionados.

Desarrollo de soluciones personalizadas

Creamos soluciones a medida para satisfacer las necesidades específicas de cada cliente, asegurando que estén preparados para enfrentar las amenazas más avanzadas.

Análisis de Inteligencia

Utilizamos técnicas avanzadas de análisis de inteligencia para proporcionar información valiosa y accionable sobre las amenazas, permitiendo a las organizaciones tomar decisiones informadas.

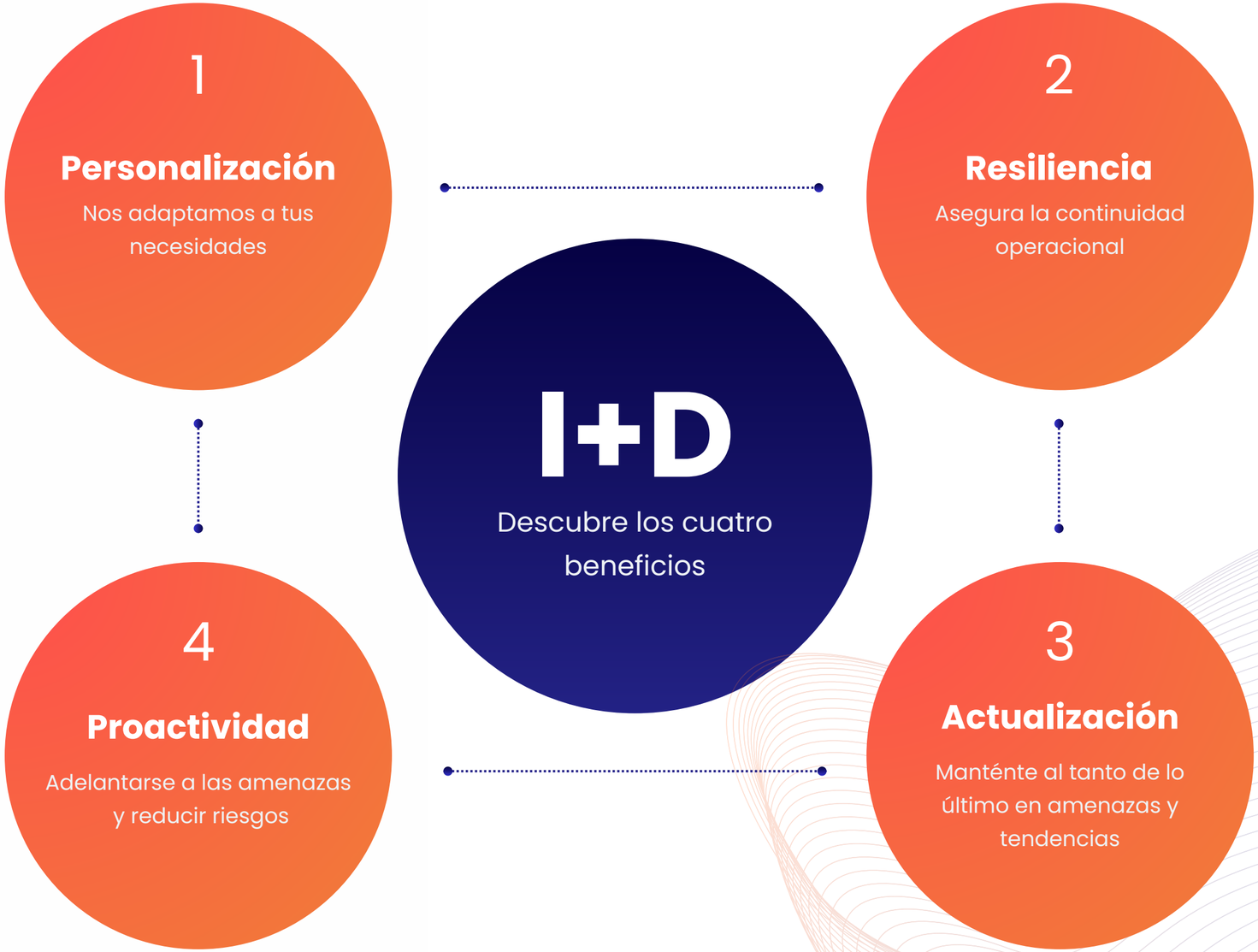
Monitoreo Continuo

Implementamos sistemas de monitoreo continuo que permiten detectar y responder a amenazas en tiempo real, minimizando el impacto potencial.

2.

Cyber Intelligence I+D

La ciberinteligencia es un pilar clave para toda organización actual.



Ethical Hacking

El pentesting -o pruebas de penetración- es un proceso de evaluación de la seguridad informática, que se realiza con el fin de identificar y explotar vulnerabilidades en redes computacionales.

En un pentesting, se simula un ataque por parte de un ciberdelincuente, con el fin de evaluar la seguridad y determinar las posibles vulnerabilidades que explotaría un ciberatacante para realizar fraudes, robos de información sensible o dejar disponible un servicio de la organización.

Objetivos

- Investigación avanzada
- Evaluar la seguridad
- Validar defensas
- Probar incidentes de seguridad
- Mapear la superficie de ataque
- Medir riesgos
- Recomendar mitigaciones

3.

Tipos de Ethical Hacking

Ethical Hacking Web / API

El objetivo de este tipo de Ethical Hacking es identificar vulnerabilidades y debilidades de seguridad en las aplicaciones web antes de que los ciberdelincuentes sean capaces de descubrirlas y explotarlas. Utilizando las últimas herramientas y técnicas utilizadas por actores maliciosos y hackers.

Ethical Hacking Mobile iOS / Android / ArmonyOS

Este tipo de Ethical Hacking se centra en dispositivos móviles, como teléfonos inteligentes y tablets, para evaluar su seguridad y detectar posibles vulnerabilidades. Estas pruebas se realizan con el consentimiento del propietario del dispositivo y tienen como objetivo identificar y solucionar problemas de seguridad antes de que puedan ser explotados por atacantes malintencionados.

4.

Ethical Phishing & Smishing

Ejercicios de Phishing

En Twoko, ofrecemos un servicio de Ethical Phishing que simula ataques de correos maliciosos reales, con el propósito de educar a los empleados y mejorar la seguridad de la organización. Estos ejercicios pueden contemplar diferentes objetivos, como obtención de datos personales, credenciales de acceso o descargas de archivos.

Ejercicios de Smishing

Los ejercicios controlados de smishing, consisten en una variante del phishing que utiliza mensajes de texto (SMS) para intentar obtener información confidencial de las víctimas. Al incluir smishing en nuestras pruebas, proporcionamos una cobertura más amplia y efectiva de las posibles amenazas de ingeniería social que su organización puede enfrentar.

5.

Análisis de vulnerabilidades

Un análisis dinámico consiste en asegurarte de que el código de tu aplicación funciona de manera segura.

Se llama dinámico debido a que se realizan las pruebas cuando este se está ejecutando, simulando la operación del programa para evaluar su comportamiento, con la finalidad de entender el comportamiento de la aplicación lo que permite levantar hallazgos de seguridad.

6.

Operaciones de Red Team

Las operaciones de Red Team sirven para evaluar la capacidad de la organización para detectar, contener, mitigar y prevenir ataques a la red, de los equipos de ciberseguridad de una organización, mediante las últimas técnicas de explotación de vulnerabilidades de seguridad y obtención de información confidencial.

twoko

Offensive Prevention

¡Hablemos!

sales@twoko.io

twoko.io

Santiago, Chile