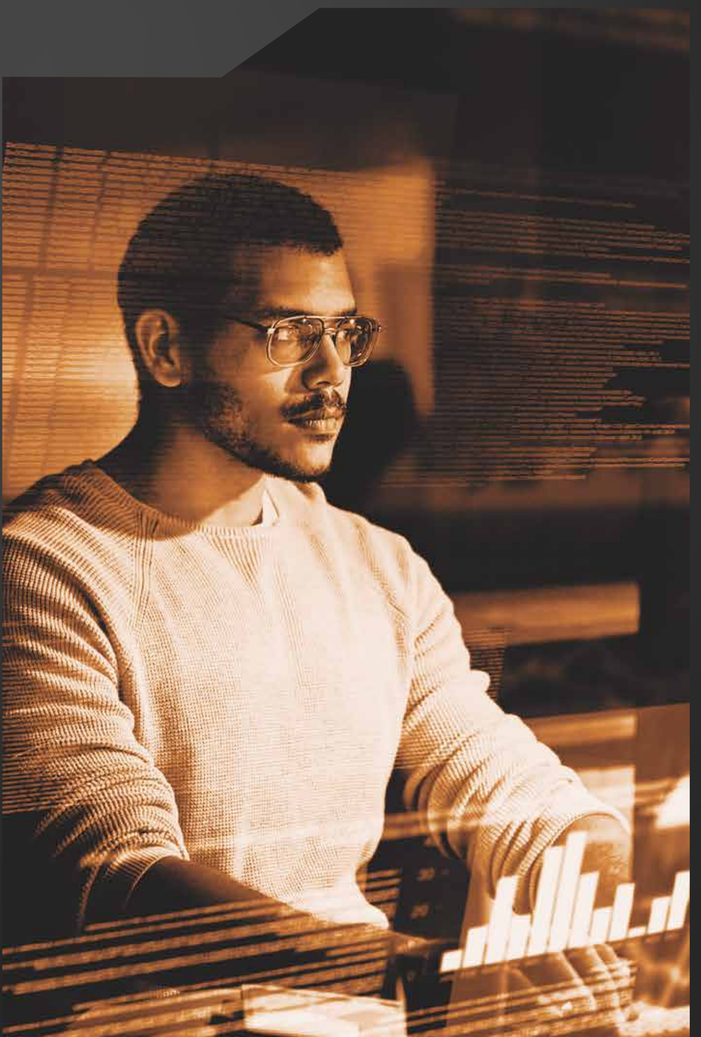
BASE4
SECURITY

Tu ciber aliado



OFFENSIVE

Una inversión segura con metodologías avanzadas y enfoques creativos

DIFERENCIALES

OSCP · OSCE · OSWP · OSWE · OSED · eCPPT v2 · eWPTX v2 · eMAPT · CEH Certified Ethical Hacker

01

+1.000 proyectos ejecutados de forma manual

02

+20.000 GAPs y amenazas encontradas

03

+500 clientes satisfechos

04

Conocimientos de redes industriales y IoT, y frameworks-MITRE/OWASP

Purple Team

Defensa y ataque en perfecta sincronía. Purple Team es un servicio colaborativo que simula ciberataques en un entorno controlado, combinando técnicas ofensivas y defensivas para evaluar la preparación y la capacidad de respuesta de tu organización en tiempo real

PROCESO

- Planificación de ejercicios: Definimos alcance y objetivos de las simulaciones
- Ataques controlados: Red Team emula adversarios, mientras el Blue Team responde
- Retroalimentación estratégica: Se comparten los resultados y se ajustan procesos de forma colaborativa

CARACTERÍSTICAS DESTACADAS

- Simulaciones controladas lideradas por nuestro Red Team, imitando ciberataques reales
- Respuesta activa del Blue Team, identificando y mitigando los ataques en tiempo real
- Análisis post-ejercicio, donde se comparten hallazgos, lecciones aprendidas y se diseñan estrategias de mejora

¿Por qué contratar ester servicio?

- Identificación de brechas de seguridad: Detectamos puntos débiles y mejoras necesarias en tus defensas
- Evaluación realista: Simulamos tácticas y procedimientos (TTP) reales para un diagnóstico práctico
- Mejora continua y aprendizaje mutuo: Fomentamos una cultura de seguridad proactiva con cada ejercicio

Contáctanos

Continuous Pentesting

Seguridad constante, adaptación continua. Implementamos un enfoque dinámico y proactivo que se diferencia del pentesting tradicional. Este servicio realiza pruebas de forma continua y sistemática, adaptándose rápidamente a los cambios en el entorno y las amenazas emergentes

PROCESO

- Evaluación inicial y setup: Definimos alcance y objetivos
- Pentesting automatizado y manual: Pruebas continuas en aplicaciones y sistemas
- Entrega de informes periódicos: Estado de seguridad, riesgos y planes de acción

CARACTERÍSTICAS DESTACADAS

- Monitoreo constante mediante tecnologías avanzadas y técnicas automatizadas
- Experiencia combinada: Análisis profundo y estratégico realizado por expertos en seguridad
- Informes regulares y en tiempo real, con vulnerabilidades detectadas y recomendaciones de mitigación

¿Por qué contratar ester servicio?

- Identificación y remediación en tiempo real: Detectamos vulnerabilidades antes de que sean explotadas por atacantes
- Integración continua en el ciclo de desarrollo: Mejoramos la seguridad a lo largo del desarrollo del software e infraestructura
- Cumplimiento de normativas: Adaptación a los estándares y regulaciones más exigentes

Contáctanos

Adversarial Emulation

Enfrenta amenazas como lo haría un atacante real. Nuestro servicio de Adversarial Emulation permite evaluar la capacidad de tu organización de resistir ciberataques específicos y conocidos. Mediante operaciones ofensivas controladas, simulamos las técnicas, tácticas y procedimientos (TTP) utilizados por actores de amenazas reales, ayudando a fortalecer la postura de seguridad y anticipar posibles riesgos

PROCESO

- Evaluación del entorno: Identificación de los adversarios más probables y relevantes
- Simulación de ataques: Reproducción de TTPs usados por actores reales para probar la defensa
- Informe y recomendaciones: Reporte con vulnerabilidades detectadas y mejoras sugeridas

CARACTERÍSTICAS DESTACADAS

- Análisis basado en los actores de amenazas más relevantes para tu sector
- Informe detallado con hallazgos y recomendaciones específicas
- Operaciones ofensivas seguras y controladas, minimizando el impacto en la producción

¿Por qué contratar ester servicio?

- Detección preventiva: Identificamos y corregimos vulnerabilidades antes de que sean explotadas
- Simulación realista: Recreamos los ataques más probables para tu organización basándonos en amenazas específicas del sector.
- Fortalecimiento proactivo: Ofrecemos recomendaciones accionables para mejorar la defensa contra adversarios potenciales.

Contáctanos

Digital Footprint

Mapea y protege tu huella digital. Nuestro servicio de Digital Footprint ofrece una visión integral de la presencia digital de tu organización a través de técnicas avanzadas de OSINT (Open Source Intelligence). Esta solución de seguridad ofensiva permite identificar riesgos ocultos y posibles vectores de ataque, evaluando tanto la exposición de información sensible como el impacto reputacional

PROCESO

- Recolección y análisis: Exploración en web pública, Deep y Dark Web, y otras fuentes relevantes
- Identificación de riesgos: Detección de vectores de ataque e información filtrada
- Informe de resultados: Entrega de un reporte con riesgos encontrados y medidas de mitigación

CARACTERÍSTICAS DESTACADAS

Investigación avanzada realizada por expertos con experiencia en OSINT

Detección temprana de información expuesta para prevenir ataques

Reportes detallados con hallazgos clave y recomendaciones accionables

¿Por qué contratar ester servicio?

- Análisis exhaustivo de fuentes abiertas (web, foros, redes sociales, repositorios, Deep y Dark Web)
- Identificación de vectores de ataque y datos sensibles expuestos
- Evaluación del riesgo reputacional y detección de oportunidades para mitigar amenazas

Contáctanos

Malware Emulation

Simulación avanzada de amenazas. Malware Emulation es un servicio especializado que permite evaluar la capacidad de tus sistemas para resistir ataques de malware avanzado, como ransomware y spyware, en un entorno controlado y seguro

PROCESO

- Diseño de malware personalizado: Adaptado a las amenazas más relevantes para tu organización
- Simulaciones en entornos seguros: Evaluamos cómo responden tus sistemas ante ataques reales
- Informe de resultados: Incluye análisis detallado y recomendaciones para fortalecer tu seguridad.

CARACTERÍSTICAS DESTACADAS

Simulación controlada de malware: Emulamos ataques reales para evaluar los niveles de protección

Análisis detallado de la efectividad de los controles de seguridad implementados

Informe técnico exhaustivo, con resultados, técnicas utilizadas y sugerencias de mejora

¿Por qué contratar ester servicio?

- Identificación de vulnerabilidades críticas: Descubrimos puntos débiles que podrían ser explotados por malware real
- Evaluación exhaustiva de defensas: Probamos la efectividad de soluciones como antivirus, firewalls, EDRs y sistemas de detección de intrusiones
- Mejora continua de la seguridad: Ofrecemos recomendaciones personalizadas para optimizar los controles y procesos

Contáctanos

Application Pentesting Manual

Asegura tus aplicaciones críticas. Evaluamos detalladamente la seguridad de tus aplicaciones web, móviles y APIs, utilizando técnicas avanzadas de pruebas de penetración. Simulamos ataques reales en entornos controlados para detectar vulnerabilidades y errores críticos que podrían comprometer tu negocio

PROCESO

- Planificación y definición de alcance: Identificación de aplicaciones críticas
- Ejecución de pruebas: Simulación de ciberataques controlados
- Informe y recomendaciones: Análisis de riesgos y plan de mitigación detallado

CARACTERÍSTICAS DESTACADAS

- Cobertura completa: Evaluaciones manuales de web, APIs y aplicaciones móviles
- Simulación de ataques controlados para entender el comportamiento real de las amenazas
- Informe con un roadmap de mitigación priorizado, facilitando decisiones estratégicas

¿Por qué contratar ester servicio?

- Descubrimiento de vulnerabilidades ocultas: Detectamos fallos que podrían pasar desapercibidos en evaluaciones tradicionales
- Análisis detallado y priorizado: Entregamos informes con hallazgos críticos y recomendaciones prácticas
- Protección integral: Probamos desde código y configuraciones hasta prácticas de seguridad para asegurar cada capa de tu aplicación

Contáctanos

Red Team Exercise

Pone a prueba tu resiliencia con simulaciones realistas. Nuestro servicio de Red Team Exercise se enfoca en realizar infiltraciones estratégicas en la infraestructura de tu organización para simular ataques avanzados. A través de una combinación de técnicas de ataque, ingeniería social y emulación de adversarios, evaluamos la capacidad de tus sistemas para resistir ciberataques reales

PROCESO

- Planificación: Definición de escenarios y objetivos estratégicos
- Ejecución del ataque: Infiltración controlada en sistemas y activos críticos
- Informe de resultados: Análisis de vulnerabilidades y recomendaciones claras para mitigación

CARACTERÍSTICAS DESTACADAS

- Simulaciones realistas alineadas con tácticas de adversarios reales
- Análisis exhaustivo de controles técnicos y operativos
- Informe detallado con hallazgos críticos y un roadmap de mejora priorizada

¿Por qué contratar ester servicio?

- Identificación de brechas críticas: Descubrimos vulnerabilidades y fallas que podrían ser explotadas
- Recomendaciones accionables: Proveemos sugerencias priorizadas para fortalecer tu plan de seguridad
- Prueba integral de controles: Evaluamos la prevención, detección, recuperación y respuesta de tu organización

Contáctanos

Social Engineering

Refuerza tu primera línea de defensa. Evaluamos la preparación de tu organización ante ataques de Phishing, Smishing y Vishing mediante la simulación controlada de estos escenarios. Nuestro objetivo es identificar vulnerabilidades humanas y mejorar la concientización en ciberseguridad del personal a través de pruebas realistas que reflejan las tácticas actuales utilizadas por los ciberdelincuentes

PROCESO

- Diseño del escenario: Creación de ataques simulados alineados con amenazas actuales
- Ejecución del ataque: Lanzamiento de campañas controladas para evaluar la respuesta
- Informe y capacitación: Recomendaciones personalizadas y, opcionalmente, charlas para cerrar las brechas detectadas

CARACTERÍSTICAS DESTACADAS

- Análisis del comportamiento del personal con indicadores de madurez
- Informes detallados con fortalezas, debilidades y recomendaciones específicas
- Simulaciones realistas de Phishing, Smishing y Vishing

¿Por qué contratar ester servicio?

- Detección de vulnerabilidades culturales: Identificamos áreas de mejora en la respuesta de los colaboradores
- Escenarios personalizados: Adaptamos los ataques simulados según las amenazas más relevantes para tu sector
- Concientización activa: Acompañamiento opcional en la estrategia de capacitación a través de charlas virtuales y presenciales

Contáctanos

Pentest Cloud | IT OT Infrastructure

Evaluación integral de vulnerabilidades. Identifica y evalúa vulnerabilidades en la infraestructura tecnológica de tu organización, cubriendo entornos de información tecnológica (IT), tecnología operativa (OT) y nube, con un enfoque proactivo y exhaustivo

PROCESO

- Simulación de ataques reales: Emulación de tácticas que los atacantes emplearían en entornos IT, OT y Cloud
- Análisis de infraestructura crítica: Evaluamos componentes clave, como servidores, redes y aplicaciones
- Informe exhaustivo y priorizado: Detalle de hallazgos y recomendaciones de mitigación

CARACTERÍSTICAS DESTACADAS

- Recopilación de datos y planificación: Identificamos el alcance y definimos los objetivos de la prueba
- Pruebas de penetración avanzada: Simulamos ataques reales en los diferentes componentes
- Análisis de riesgos: Evaluamos el impacto y la probabilidad de cada vulnerabilidad encontrada
- Informe y recomendaciones: Generamos un análisis detallado con pasos prioritarios para mejorar la seguridad.

¿Por qué contratar ester servicio?

- Descubrimiento de fallos de seguridad: Identificamos y evaluamos configuraciones incorrectas y vulnerabilidades explotables
- Visión integral de la postura de seguridad: Proporcionamos una evaluación completa de la infraestructura
- Prevención proactiva de amenazas: Ayudamos a mitigar riesgos antes de que se conviertan en incidentes

Contáctanos

¿Por qué elegir BASE4 Security?

> **Garantía de servicio**
Brindamos una medida de seguridad y confianza en la calidad de nuestros servicios de ciberseguridad.

> **Respaldo de talentos con renombre global**
Nuestra cultura empresarial, certificada y premiada, es elegida por personas de alto nivel y reconocimiento técnico.

> **Servicio consultivo**
Ofrecemos soluciones adaptadas al cliente para abordar los desafíos o necesidades específicas en materia de ciberseguridad.

BASE4
SECURITY

www.base4sec.com