

SH13LD-4CE



SHIELD FORCE RED TEAM



¿Cuál es el costo para el negocio?

- Cuando los servicios no estén disponibles
- Por el acceso y cambios no autorizados
- Por la alteración a información o bases de datos
- Por el robo de información sensible o crítica
- Por la fuga de información confidencial
- Por una negación / interrupción del servicio
- Por la pérdida de la confianza del cliente por fallas del sistema

Servicios Profesionales

Servicios RED TEAM

Consiste en ejecutar servicios controlados que identifiquen amenazas y potenciales riesgos, confirmando los que puedan ser explotados, clasificando y priorizando las amenazas y vulnerabilidades que puedan impactar las operaciones y el negocio. Así mismo es demostrar como un usuario malicioso no autorizado puede lograr ganar acceso explotando vulnerabilidades para establecer estrategias e iniciativas de mejora y de ser posible erradicar y fortalecer su infraestructura operacional.

Los servicios son entregados basados en estándares de la industria:



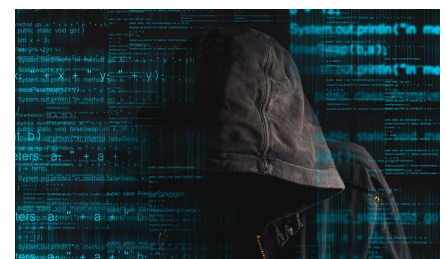
Equipo Rojo

Servicios que entregamos:

- Simulación de Adversario Malicioso
- Pruebas de Ejecución Blue Team / Red Team
- Análisis de Vulnerabilidades y Pruebas de Penetración
 - Infraestructura de Red
 - Redes Inalámbricas
 - Servidores / Estaciones de Trabajo
 - Bases de Datos
 - Aplicación Web
 - Aplicación Móvil
 - Código Dinámico
 - Código Estático
- Pruebas de Ingeniería Social

Modalidades

- Caja Negra / Caja Gris / Caja Blanca
- Externo (Internet)
- Interno (En sitio)
- Única Vez
- Mensual / Trimestral / Semestral / Anual

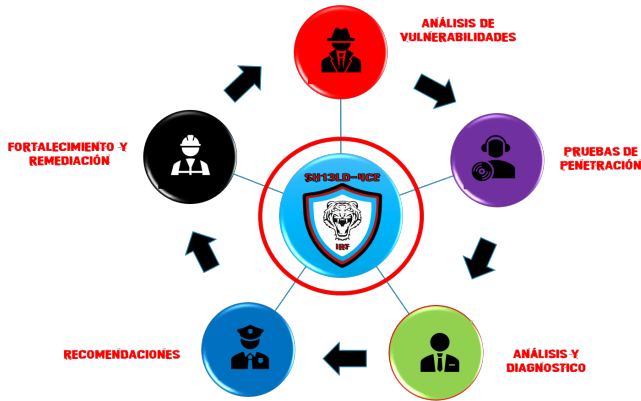


Proceso de Análisis de Vulnerabilidades y Pruebas de Penetración

Nuestros especialistas planean y ejecutan las tareas de análisis de vulnerabilidades y pruebas de penetración usando herramientas comerciales y “Open Source” como Veracode, Immuniweb, Acunetix, Tenable, Kali Linux, Metasploit.

Se determina el alcance, enumeran vulnerabilidades que se analizan para realizar la explotación de aquellas que sea posible, a fin de ganar acceso, escalar privilegios y realizar el ataque.

Nuestros consultores siguen reglas para hacer del estudio un valor y no un riesgo. Posteriormente se realiza la limpieza y se restauran las operaciones para realizar el reporte de hallazgos.



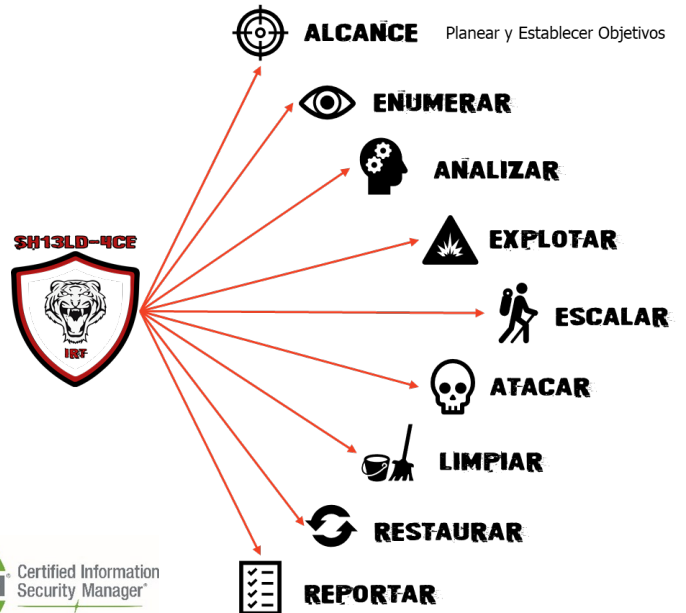
Análisis y Diagnóstico: Se obtienen los resultados de las herramientas, se documentan los hallazgos que representan riesgos o amenazas potenciales y se clasifican y ponderan las vulnerabilidades siendo el “driver” el negocio, también analizamos las vulnerabilidades, amenazas e impacto en las operaciones

Recomendaciones: Realizamos un reporte de recomendaciones de mejora sobre los hallazgos a fin de que el cliente pueda realizar las actividades de mejora.

Fortalecimiento y Remediación: Podemos realizar el acompañamiento con el cliente para la mejora y fortalecimiento de las vulnerabilidades encontradas, así mismo podemos apoyar al cliente a realizar las actividades de fortalecimiento, con el fin de remediarnos.


Entregables

- Reportes de las herramientas (as is) en “bruto”
- Reporte de Vulnerabilidades encontradas, priorizando el impacto en las operaciones
- Reporte de lo que se logro “explotar” en las pruebas de penetración
- Reporte de Recomendaciones de Fortalecimiento
- Reporte del Proceso de fortalecimiento (Si aplica)
- Bitácora de actividades



Certificaciones de nuestros consultores





SHIELD FORCE
www.shieldforce.mx

ventas@shieldforce.mx
+52.55.53.51.15.56
ext. 2010

INCIDENT RESPONSE TEAM
S.A. DE C.V.
Insurgentes Sur 1458 Piso 19,
Col. Actipan, Alcaldía Benito Juárez,
03230, Ciudad de México.