



Servicio Red Team

Cliente

Banca
Dimensión: 20.000
Presencia Global

Desafío

El cliente buscaba mejorar su postura de seguridad y sus protocolos de respuesta para defenderse mejor de las ciberamenazas, como los ataques selectivos o el ransomware. Su objetivo era identificar los puntos débiles de sus sistemas y procesos.

Solución

Proporcionamos un servicio de Equipo Rojo que cubría diferentes tácticas, técnicas y procedimientos (TTP) emulando ataques dirigidos y ransomware. Durante el ejercicio, nuestro equipo llevó a cabo diversas actividades para recopilar información sobre la superficie de ataque expuesta del cliente.

Las acciones de intrusión se desencadenaron desde el exterior mediante ingeniería social y explotación técnica de vulnerabilidades, culminando el ejercicio con la persistencia y exfiltración de datos.

Tras la ejecución del ejercicio, proporcionamos una descripción detallada de las acciones realizadas, las rutas de ataque utilizadas y las vulnerabilidades explotadas para que el cliente pudiera analizar y mejorar la postura global, incluidos los procesos de detección y respuesta.

Durante el proceso, trabajamos con el equipo SOC/Blue del cliente para ayudar a identificar los puntos ciegos y a evaluar las mejoras implementadas tras el ejercicio.

Impacto

El cliente conoce ahora mejor la superficie de ataque expuesta, los puntos débiles de la infraestructura tecnológica y los procesos que la sustentan. Dado que el ejercicio se llevó a cabo sin el conocimiento general de la organización, el cliente tuvo la oportunidad de evaluar de forma realista el rendimiento de su SOC y aplicar medidas que condujeron a una mayor resistencia a los ciberataques, reduciendo considerablemente el riesgo para la organización.

Servicios Relacionados

- Red Teaming

Making your tech journey **more secure.**

For more information, please visit

www.integrity.pt