Caso 4: OSINT y Superficie de Ataque

Nota: Documento demostrativo (caso hipotetico/anonimizado)
No contiene datos reales de clientes.

RESUMEN EJECUTIVO
Evaluacion de superficie de ataque mediante tecnicas OSINT
identificando activos expuestos y vectores potenciales de compromiso.

ALCANCE
- Reconocimiento pasivo de dominios y subdominios
- Identificacion de activos en nube publica
- Busqueda de credenciales filtradas
- Analisis de metadatos en documentos publicos
- Evaluacion de presencia en redes sociales corporativas

HALLAZGOS PRINCIPALES
ALTA: Credenciales de empleado en breach publico
ALTA: Subdominio staging expuesto sin autenticacion
MEDIA: API keys en repositorio publico historico
MEDIA: Servidor de desarrollo indexado en Shodan

ENTREGABLES
- Inventario completo de activos digitales expuestos
- Mapa de superficie de ataque visual
- Listado de subdominios y servicios descubiertos
- Reporte de credenciales comprometidas

RESULTADOS
Reduccion del 65% de superficie de ataque en 60 dias.
12 activos criticos removidos de exposicion publica.