Checklist de alcance PenTest

Talsoft TS

Checklist de alcance PenTest - Talsoft TS

Usar este checklist antes de pedir una propuesta de Penetration Testing. Sirve para ordenar objetivo, activos, permisos, ventana y capacidad de remediacion. No reemplaza una conversacion de alcance, un diagnostico GAP, readiness ni gestion continua de riesgo. Un PenTest no garantiza ausencia de vulnerabilidades ni ausencia de incidentes.

1. Objetivo de negocio:

- Que presion origina el PenTest: cliente enterprise, auditoria, ciberseguro, re-test, incidente, roadmap o validacion tecnica.
- Que decision debe habilitar el resultado.
- Que evidencia espera recibir la contraparte.
- Que fecha limite existe y por que.

2. Activos dentro de alcance:

- URLs, aplicaciones, APIs, dominios, rangos, entornos cloud, mobile o infraestructura.
- Ambiente objetivo: produccion, staging, testing o laboratorio.
- Dependencias relevantes: proveedores, terceros, autenticacion, integraciones y datos sensibles.
- Activos excluidos y motivo.

3. Permisos y reglas de engagement:

- Responsable interno que aprueba el alcance.
- Autorizacion escrita para ejecutar la prueba.
- Ventana de prueba, huso horario y restricciones operativas.
- Contacto tecnico disponible durante la ejecucion.
- Canales para incidentes, pausas o dudas de alcance.

4. Credenciales y accesos:

- Tipo de prueba: caja negra, gris o blanca.
- Usuarios, roles y permisos disponibles.
- Reglas para MFA, bloqueo de cuentas, rate limits y alertas.
- Datos de prueba permitidos y datos que no deben tocarse.

5. Capacidad de remediacion:

- Equipo responsable de corregir hallazgos.
- Criterio para priorizar severidad, impacto y exposicion.
- Plazos realistas para correccion.
- Necesidad de re-test y evidencia posterior.

6. Entregables esperados:

- Resumen ejecutivo.

- Reporte tecnico con hallazgos priorizados.
- Roadmap inicial de remediacion.
- Evidencia para cliente, auditoria o ciberseguro si aplica.
- Re-test o seguimiento segun alcance.

7. Senales de que conviene empezar por GAP:

- No esta claro que activos son criticos.
- No hay owner interno para aprobar alcance y remediar.
- La empresa no sabe que evidencia existe.
- La presion externa mezcla auditoria, cliente, ciberseguro y controles generales.
- El objetivo es ordenar postura, no solo validar exposicion tecnica.

8. Lo que no debe prometerse:

- No garantiza ausencia de vulnerabilidades.
- No garantiza ausencia de incidentes.
- No reemplaza un programa de madurez ni readiness.
- No debe ejecutarse sin autorizacion, reglas de engagement y alcance aprobado.

Siguiente paso sugerido:

- Si el alcance, permisos y remediacion estan claros, preparar una conversacion de PenTest.
- Si el alcance o ownership no estan claros, empezar por Initial GAP + Roadmap o una conversacion ejecutiva.