PenTest scope checklist

Talsoft TS

PenTest scope checklist - Talsoft TS

Use this checklist before requesting a Penetration Testing proposal. It helps organize objective, assets, permissions, test window and remediation capacity. It does not replace a scope conversation, GAP assessment, readiness or ongoing risk management. A PenTest does not guarantee absence of vulnerabilities or absence of incidents.

1. Business objective:

- What pressure triggered the PenTest: enterprise customer, audit, cyber insurance, re-test, incident, roadmap or technical validation.
- What decision the result should enable.
- What evidence the third party expects.
- What deadline exists and why.

2. Assets in scope:

- URLs, applications, APIs, domains, ranges, cloud environments, mobile or infrastructure.
- Target environment: production, staging, testing or lab.
- Relevant dependencies: vendors, third parties, authentication, integrations and sensitive data.
- Excluded assets and reason.

3. Permissions and rules of engagement:

- Internal owner approving the scope.
- Written authorization to execute the test.
- Test window, timezone and operational restrictions.
- Technical contact available during execution.
- Channels for incidents, pauses or scope questions.

4. Credentials and access:

- Test type: black box, gray box or white box.
- Users, roles and permissions available.
- Rules for MFA, account lockout, rate limits and alerts.
- Test data allowed and data that must not be touched.

5. Remediation capacity:

- Team responsible for fixing findings.
- Criteria to prioritize severity, impact and exposure.
- Realistic correction timelines.
- Need for re-test and follow-up evidence.

6. Expected deliverables:

PenTest scope checklist

Talsoft TS

- Executive summary.
- Technical report with prioritized findings.
- Initial remediation roadmap.
- Evidence for customer, audit or cyber insurance if applicable.
- Re-test or follow-up based on scope.

7. Signals that GAP should come first:

- Critical assets are unclear.
- There is no internal owner to approve scope and remediate.
- The company does not know what evidence exists.
- External pressure mixes audit, customer, cyber insurance and general controls.
- The objective is to organize posture, not only validate technical exposure.

8. What should not be promised:

- It does not guarantee absence of vulnerabilities.
- It does not guarantee absence of incidents.
- It does not replace a maturity program or readiness.
- It should not run without authorization, rules of engagement and approved scope.

Suggested next step:

- If scope, permissions and remediation are clear, prepare a PenTest scope conversation.
- If scope or ownership is unclear, start with Initial GAP + Roadmap or an executive conversation.