
REDSEC
LABS
Penetration Testing Pricing Document
Commercial in Confidence

Contents

Penetration Testing Pricing

Pricing Summary

All pricing is subject to scoping, discovery and environment review.

Penetration Testing delivered by RedSecLabs is tailored to each organisation's environment, regulatory obligations and operational complexity. Engagements are priced on a day-rate basis that reflects the level of expertise required, the risk profile of the systems being assessed, and the depth of testing necessary for assurance.

The number of days required for each penetration test depends on:

- the type of test requested (infrastructure, application, cloud, red team, mobile etc.)
- the size and complexity of the environment
- the maturity of the client's security controls
- whether PCI DSS, DORA, or other regulatory requirements apply
- any specific cloud or identity constraints (Azure AD, AWS IAM, GCP IAM, M365, Zero Trust, hybrid environments)

RedSecLabs offers a tiered pricing model that reflects the complexity and skill level required to deliver each engagement. This structure is aligned with the model presented in the reference document, adapted for RSL's penetration testing specialisation.

RedSecLabs (RSL) Penetration Testing Day Rates

Level	Strategy & Architecture	Change & Transformation	Development & Implementation	Delivery & Operation	People & Skills	Relationships & Engagement
1. Follow	–	–	–	–	–	–
2. Assist	–	–	–	–	–	–
3. Apply	£900	£900	£900	£900	£900	£900
4. Enable	£1050	£1,050	£1,050	£1,050	£1,050	£1,050
5. Ensure, Advise	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250
6. Initiate, Influence	£1,350	£1,350	£1,350	£1,350	£1,350	£1,350
7. Set Strategy, Inspire, Mobilise	£1,450	£1,450	£1,450	£1,450	£1,450	£1,450

What the tiers represent (RSL-specific clarifications):

- **Apply (Level 3)** – Standard penetration testing activities (web apps, APIs, external infrastructure, internal testing).
- **Enable (Level 4)** – Specialist penetration testing including cloud exploitation, identity assessments (Azure AD / AWS IAM), advanced AD exploitation, and mobile application testing.
- **Ensure & Advise (Level 5)** – PCI DSS QSA-aligned testing, DORA-aligned resilience testing, infrastructure deep-dive assessments, and engagements requiring multi-engineer collaboration.
- **Initiate & Influence (Level 6)** – Red Teaming, adversary simulation, multi-vector testing, and highly complex or sensitive penetration testing requiring senior consultants.
- **Set Strategy, Inspire, Mobilise (Level 7)** – Executive advisory support, strategic testing oversight, CISO-level governance alignment, regulatory testing programmes, and testing requiring senior-level sign-off for regulated industries.

Pricing Assumptions

- An initial scoping exercise or questionnaire must be completed. Based on this, RedSecLabs will recommend the required number of days for the engagement.
- Pricing is provided on a fixed-price basis aligned with the agreed scope of days.
- A formal Statement of Work (SoW) will be issued prior to commencement, outlining scope, testing boundaries, methodology, reporting requirements and key milestones.
- Any changes to scope, requirements or assumptions will be managed under change control and may incur additional costs where extra days are required beyond those initially agreed.
- Certain types of engagements — such as Red Teaming, PCI DSS CDE segmentation testing, cloud identity exploitation, Azure AD/OAuth abuse analysis and DORA resilience testing — may require higher-tier pricing based on seniority and risk.
- Work is delivered remotely unless otherwise agreed; on-site work may incur additional expenses (travel, logistics, secure testing hardware).
- All testing is conducted subject to safe-exploitation guidelines and legal constraints defined in the Rules of Engagement (RoE).