REDSEC LABS

PENETRATION TESTING

Service Definition Document

Contents

1. Solution Overview

RedSecLabs delivers a comprehensive suite of penetration testing services designed to help organisations evaluate, strengthen and continuously improve the resilience of their digital landscape. Our testing methodology is deeply grounded in real-world adversarial behaviour and draws upon established frameworks including NIST 800-115, OWASP, MITRE ATT&CK and CREST-aligned practices. This ensures every engagement provides a highly contextual, evidence-driven understanding of risk.

Our services are engineered to support organisations operating in regulated sectors such as finance, telecommunications, health, e-commerce and government, where compliance requirements are stringent and security expectations are high. The testing approach fully aligns with GDPR, PCI DSS, DORA, ISO 27001 and similar governance frameworks, helping clients maintain regulatory assurance while bolstering their internal cyber controls.

Each engagement is conducted by experienced penetration testers with strong offensive security backgrounds, practical cloud-security expertise and PCI DSS QSA exposure. RedSecLabs blends methodical analysis with controlled exploitation to identify vulnerabilities, reveal privilege-escalation paths, and demonstrate how weaknesses may be chained together to create real business impact.

2. What is Penetration Testing?

Penetration Testing is a controlled and authorised simulation of advanced cyberattacks performed with the objective of identifying, exploiting and validating weaknesses across an organisation's digital ecosystem. Unlike routine vulnerability scanning, penetration testing adopts the mindset and behaviour of a threat actor, combining reconnaissance, exploitation, evasion, privilege escalation, identity abuse and cloud misconfiguration analysis.

Through this approach, RedSecLabs helps organisations understand how adversaries might compromise critical systems, disrupt business processes or exfiltrate sensitive information. The assessment extends beyond finding isolated technical issues and instead provides a realistic, end-to-end view of how a motivated attacker could progress through the environment.

Our testing strictly adheres to legal and ethical requirements, including the mandatory evidence-handling, scoping and reporting standards defined within PCI DSS penetration testing procedures and GDPR Article 32 expectations. This ensures clients receive rigorous, defensible security assurance suitable for both internal leadership and external regulatory bodies.

3. Key Features

RedSecLabs' penetration testing service offering covers a mature and diverse range of offensive security disciplines. While tightly focused on penetration testing, the service maintains broad visibility across infrastructure, cloud, identity, applications and user interaction flows. Each engagement is tailored to the client's technology stack, operational environment, regulatory exposure and risk appetite.

Key features of RedSecLabs' penetration testing services include:

- **Realistic adversary simulation** grounded in MITRE ATT&CK and CREST-aligned methodologies.
- **Deep manual testing**, extending beyond automated tools and signatures.
- **Hybrid cloud expertise** covering AWS, Azure, GCP, M365 and identity platforms.
- **Business logic and API exploitation**, not just technical vulnerability testing.
- **Privilege escalation and lateral movement analysis** for infrastructure engagements.
- **Zero-trust resilience testing**, particularly for organisations using modern identity-driven architectures.
- **Evidence-driven exploitation**, ensuring each vulnerability is demonstrated with practical impact where safe and permitted.

This approach ensures each organisation receives assurance that is technically rigorous, operationally relevant and aligned to industry expectations such as those within PCI DSS, GDPR, DORA and ISO 27001.

4. Key Benefits

A penetration test conducted by RedSecLabs provides decision-makers with clarity, confidence and actionable insights into the real security posture of their environment. The findings not only highlight exploitable attack paths but also help organisations understand how these weaknesses translate into actual business and operational risk.

Key benefits include:

- **Clear visibility** into the vulnerabilities most likely to be exploited by real-world attackers.
- **Validation of existing defence mechanisms**, including firewalls, IDP/MFA controls, cloud identity policies and application logic.

- **Improved cyber-resilience** through identification of systemic weaknesses such as privilege misuse, segmentation flaws or insecure coding patterns.
- **Independent third-party assurance** suitable for board reporting, audits and regulatory compliance.
- **Actionable remediation guidance**, enabling teams to implement effective and prioritised security improvements.
- **Direct support for compliance initiatives**, particularly PCI DSS, DORA operational resilience testing, GDPR security controls and ISO 27001 Annex A requirements.

5. Service Overview

The following sections outline the penetration testing services provided by RedSecLabs. Each category focuses solely on offensive security, written in detailed, professional paragraphs, with bullet points introduced only where clarity improves comprehension.

5.1 External Infrastructure Penetration Testing

External Infrastructure Penetration Testing evaluates the resilience of an organisation's internet-facing assets by simulating attacks originating from hostile actors outside the environment. The assessment begins with intelligence-led reconnaissance to identify exposed services, underlying technologies and cloud-linked dependencies. RedSecLabs then performs deep manual inspection and targeted probing to uncover weaknesses such as outdated software, weak cryptography, service misconfigurations, authentication flaws or insecure identity federation.

Where in-scope and safe to do so, RedSecLabs performs controlled exploitation to demonstrate the feasibility of compromise and highlight whether an attacker could gain a foothold, pivot into internal systems or manipulate external identity providers such as Azure AD or M365. This service provides organisations with a realistic understanding of how their perimeter appears to attackers and how susceptible it may be to modern threat vectors.

5.2 Internal Infrastructure and Active Directory Penetration Testing

Internal Infrastructure and Active Directory Penetration Testing focuses on evaluating risks that arise once an attacker gains access to the internal network—whether through compromised credentials, malware, phishing or insider behaviour. The assessment begins with the discovery of active systems, available services, and shared resources, followed by detailed enumeration of the organisation's identity infrastructure.

RedSecLabs examines trust relationships, group policy configurations, password hygiene and privilege assignment to identify lateral movement opportunities and privilege-escalation paths.

Techniques such as Kerberoasting, credential relaying, token impersonation and misconfiguration exploitation are used to determine whether a complete domain compromise is feasible. This service provides invaluable insight into structural weaknesses that could allow attackers to propagate rapidly across internal systems.

5.3 Web Application and API Penetration Testing

Web Application and API Penetration Testing involves a deep examination of customer-facing, internal and partner-facing applications to assess how securely they process, store and transmit data. RedSecLabs evaluates authentication mechanisms, session management, business logic flows, user authorisation and backend integrations, following established practices from OWASP Top 10, SANS Top 25 and CREST application testing guidelines.

The process includes thorough mapping of application functionality and an exploration of potential entry points for injection attacks, authorisation bypasses, insecure direct object references, deserialisation flaws and server-side request forgery. APIs are assessed for schema weaknesses, broken access control, insufficient rate limiting and improper handling of user input. By combining manual testing with controlled exploitation, RedSecLabs provides insight into both common vulnerabilities and complex logic flaws often missed by automated scanners.

5.4 Mobile Application Penetration Testing

Mobile Application Penetration Testing addresses the security challenges unique to mobile ecosystems. RedSecLabs evaluates Android and iOS applications through a combination of static code analysis, dynamic runtime testing and controlled reverse engineering. Local data storage, network communication, authentication flows and encryption mechanisms are assessed to determine how securely the application protects user data.

Where safe and appropriate, applications are tested on rooted or jailbroken devices to reveal vulnerabilities that attackers commonly exploit outside the normal security model. This provides organisations with a comprehensive picture of mobile application risks across both standard and compromised environments.

5.5 Cloud Security Penetration Testing

Cloud Security Penetration Testing focuses on identifying weaknesses across major cloud platforms such as AWS, Azure, GCP and M365. RedSecLabs evaluates identity and access roles, policy configurations, storage permissions, administrative interfaces, exposed APIs and network segmentation. Cloud misconfigurations remain one of the most common causes of breaches, and this assessment helps organisations understand whether weaknesses in IAM, Conditional Access, serverless components or containerised workloads could result in compromise.

Particular emphasis is placed on privilege-escalation paths, OAuth consent abuse, key mismanagement and incorrectly configured cross-tenant or multi-cloud trust relationships. This form of testing is essential for organisations working towards DORA compliance or operating within PCI DSS cardholder environments.

5.6 Red Teaming and Adversary Simulation

Red Teaming provides a broader, more holistic security assessment by replicating persistent and highly capable threat actors rather than simply identifying technical vulnerabilities. RedSecLabs uses a realistic attacker mindset to achieve defined objectives that reflect business-critical risks, such as obtaining sensitive data, bypassing identity controls or compromising key systems.

The engagement combines physical intrusion attempts, social engineering, technical exploitation and cloud attack paths to test how well an organisation can detect, respond to and contain sophisticated adversaries. The result is a comprehensive view of operational resilience, detection maturity and the effectiveness of an organisation's incident response capabilities.

5.7 Wireless Security Assessment

Wireless Security Assessment evaluates the integrity and security of wireless networks used by the organisation. RedSecLabs examines authentication protocols, encryption strength, access point configurations and guest network segregation to identify weaknesses that could allow an attacker to compromise wireless connectivity.

Controlled testing is used to assess susceptibility to rogue access point attacks, credential interception and impersonation attempts, ensuring that wireless networks are robust enough to prevent both opportunistic and targeted threats.

5.8 Vulnerability Scanning

Vulnerability Scanning provides the foundational visibility required to identify known weaknesses across an organisation's infrastructure. RedSecLabs supplements automated scanning tools with manual validation to eliminate false positives and ensure findings are accurate, prioritised and actionable. This service helps organisations maintain compliance with frameworks such as PCI DSS and ISO 27001, both of which require recurring, accurate vulnerability management practices.

6. Objectives of the Service

The primary objective of RedSecLabs' penetration testing services is to enable organisations to detect and address security weaknesses before they can be exploited by malicious actors. By

delivering realistic attack simulations, our services provide independent assurance that defence mechanisms are functioning as intended and that systems can withstand modern threats.

The assessments support compliance with frameworks such as GDPR, PCI DSS, DORA and ISO 27001, helping clients maintain regulatory alignment while strengthening operational resilience. Ultimately, the objective is to equip leadership and technical teams with clear, evidence-driven insights that support long-term security maturity and continuous improvement.

7. PCI DSS, CREST and Regulatory Alignment

RedSecLabs adheres to globally recognised penetration testing standards, with methodologies aligned to PCI DSS testing requirements, CREST infrastructure and application testing practices, and sector-specific regulatory frameworks.

- **PCI DSS QSA Experience:** Our understanding of cardholder data environments enables us to carry out segmentation validation, authentication testing and secure code assessments aligned with PCI DSS requirements.
- **CREST Alignment:** Testing methodologies follow CREST-recognised practices, ensuring technical rigour, consistency and auditability suitable for regulated sectors.
- **Regulatory Relevance:** The approach directly supports compliance with GDPR (Article 32), DORA ICT risk testing and ISO 27001 Annex A controls.

This ensures all penetration testing engagements align with both industry and regulatory expectations.

8. Broader Governance and Compliance Services

Although this document focuses on penetration testing, RedSecLabs provides a complementary suite of governance and compliance services that help organisations achieve complete security maturity. These include GDPR and Data Protection Officer services, DORA resilience assessments, PCI DSS consulting, ISO 27001 implementation, and cloud governance reviews.

By integrating governance expertise with offensive testing, RedSecLabs ensures that technical findings can be effectively embedded into organisational policies, risk registers, compliance roadmaps and long-term security strategies.

9. Engagement Deliverables

Each RedSecLabs penetration testing engagement delivers a comprehensive and structured set of outputs designed for multiple audiences. Executive summaries provide high-level insights

suitable for leadership and board members, while technical sections include detailed vulnerability descriptions, impact analysis, reproduction steps and remediation recommendations.

Reports include a consolidated severity matrix, visual diagrams where relevant, and full supporting evidence such as screenshots, network captures or exploitation walkthroughs. Where required, RedSecLabs also provides retesting services to validate that mitigation efforts have been applied correctly and effectively.

10. Reporting Structure

RedSecLabs' reporting structure is designed to be clear, consistent and auditor-friendly. Reports begin with an executive overview, followed by a description of the engagement scope, rules of engagement and testing methodology. Each finding is presented with a description, business impact, likelihood assessment, severity rating, evidence and recommended mitigation steps.

The report concludes with strategic recommendations that help organisations improve broader security maturity and align with regulatory obligations such as PCI DSS, GDPR and DORA.

11. Out-of-Scope Services

Penetration testing focuses on identifying and validating vulnerabilities, and therefore does not include remediation, architectural redesign or long-term security monitoring as part of the core service. However, RedSecLabs can provide remediation guidance, cloud security consulting, secure architecture design and Managed SOC services as part of separate engagements where ongoing support is required.

12. Team Accreditations

RedSecLabs testers hold advanced offensive and governance certifications that demonstrate deep technical capability and audit-readiness. These include OSCP, OSWE, OSEP, CREST-aligned expertise, Azure/AWS/GCP security certifications, CISSP, CISA, PCI DSS QSA experience and ISO 27001 qualifications. This blend of offensive and governance backgrounds ensures that testing is both technically rigorous and aligned with regulatory requirements and industry best practices.

13. Risk Assessment Model

RedSecLabs uses a structured and transparent risk assessment model combining CVSS v3.1 scoring, OWASP risk rating and an internally calibrated likelihood-impact matrix. This ensures each finding is evaluated in a way that reflects realistic exploitability, technical exposure and

business impact. The resulting risk profile helps organisations properly prioritise remediation efforts and align corrective actions with risk appetite, operational needs and compliance expectations.