redesign

redesign-group.com

SERVICE BRIEF

Internal Penetration *Testing*

re

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Internal Penetration Testing services. These services simulate real-world internal threats to assess and validate the effectiveness of security controls within an Customer's internal network environment.

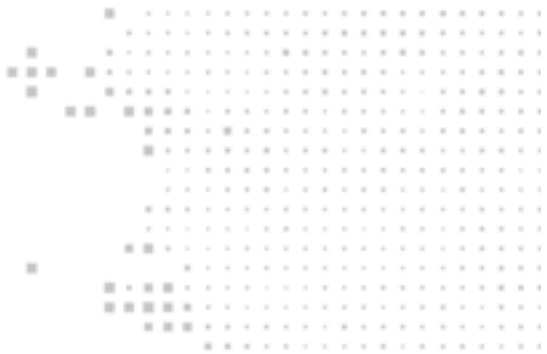
This service engagement is governed by this Service Brief and associated with SKU: SEC-PENINT.

The quantity defined in the quote determines the number of internal IPs or network segments to be tested under this engagement.

The *future* belongs
to the *curious*.

Table of Contents

01. Services Overview



Redesign's Internal Penetration Testing Services simulate the actions of a malicious insider or a compromised endpoint operating within the Customer's internal network environment. These assessments are designed to identify vulnerabilities, lateral movement opportunities, and exposure of sensitive data or administrative controls. Testing is conducted in a controlled manner intended to minimize operational impact; however, no guarantee can be made that testing activities will be entirely risk-free.

The testing process is aligned with industry standards and methodologies, including NIST SP 800-115, MITRE ATT&CK, and relevant components of the OWASP Testing Guide.

The services are divided into distinct stages:

- Pre-Engagement Planning
- Reconnaissance & Enumeration
- Vulnerability Analysis
- Exploitation & Validation
- Reporting & Close-Out

The engagement is considered complete upon delivery of the final Penetration Testing Report and completion of the Findings Review Session.

02. Offer Structure

PRIMARY SERVICES

- Includes local or remote execution of internal network testing within the defined quantity and scope of internal IPs, VLANs, or segments.

OPTIONAL ADD-ONS

Separate SOW

- Includes social engineering, physical security testing, or full red-team assessments.

03. Project Scope

This engagement focuses on simulating threats from within the network perimeter—either from a rogue employee, compromised workstation, or an attacker with internal access.

In-Scope Assets:

- **Internal IP ranges (as defined in quote/SOW)**
- **Domain controllers, user subnets, file servers, print servers, and other core infrastructure**
- **Internal web applications (basic enumeration only; no authenticated testing or business logic analysis unless explicitly scoped)**
- **Workstations (as authorized and reachable)**

Requirements:

- **Legal ownership or contractual authorization for all in-scope systems**
- **Testing must align with Customer's internal risk management and approval processes**
- **Onsite presence or secure VPN access to internal network**
- **Dedicated testing VLAN or jump host (as applicable)**
- **Test Credentials: Customer will provide test credentials or limited-access accounts for gray-box testing. Any credentials provided must be non-production and limited-privilege unless otherwise approved in writing.**

All devices must be functional, supported, and reachable for inclusion.

04. Quantity & Effort Model

- **Service SKU: SEC-PENINT**
- **Quantity: Number of internal IP addresses, subnets, or user groups covered under this engagement as defined in quote**
- **Work per Unit:**
  - Internal asset discovery and mapping
  - Vulnerability enumeration and validation
  - Lateral movement testing
  - Reporting of per-IP or per-segment findings

Example: A quantity of 250 under SKU SEC-PENINT authorizes testing of 250 internal IP addresses. Increases in quantity may require additional licensing and scope modification.

MONTHLY SUPPORT TERMS

This service includes up to the number of hours specified in the associated quote for operational support per month, limited to the activities defined in this Service Brief.

Unused hours do not carry over to subsequent months. Additional support hours may require a revised quote or a separate Statement of Work (SOW).

05. Services & Key Activities

Stage	Key Activities
Pre-Engagement Planning	▪ Confirm scope, access, and environment restrictions ▪ Finalize Rules of Engagement (ROE) ▪ Schedule testing window ▪ Validate safe testing zones and contacts
Internal Reconnaissance & Enumeration	▪ Network scanning (IP, port, service discovery) ▪ Host and service fingerprinting ▪ Active Directory enumeration (if applicable)
Vulnerability Analysis	▪ Identification of insecure services, misconfigurations, and exposed ports ▪ Manual validation of vulnerabilities ▪ Threat modeling and correlation with known exploits
Exploitation & Validation	▪ Attempt exploitation of confirmed vulnerabilities ▪ Validate access escalation paths ▪ Attempt lateral movement and data access (in a safe, controlled manner)
Reporting & Close-Out	▪ Develop and deliver Internal Penetration Testing Report ▪ Conduct findings review with Customer team ▪ Provide prioritized remediation guidance

06. Deliverables

Rules of engagement (ROE) document

Internal penetration testing report, including:

- Executive Summary
- Technical Findings with Prioritized Severity Rankings
- Proof-of-Concept Evidence
- Remediation Recommendations

Findings review session (virtual, 1 hour)

07. Services Scope Changes

Changes to the authorized IP list, schedule, or volume may result in scope or cost adjustments and require a Change Request (CR).

---

08. Services Scope Exclusions

This engagement does not include:

- **Social engineering, phishing, or vishing campaigns**
- **Physical security assessments or facility access**
- **Denial of Service (DoS) testing**
- **Ongoing vulnerability management**
- **Source code analysis**
- **Remediation assistance**
- **Workstation or mobile device testing outside the approved IP range**
- **Cloud-native internal testing (e.g., cloud control plane, IAM, native PaaS services) unless explicitly defined in scope**

---

09. Customer Responsibilities

Maintain valid vendor support agreements:

- **Access Provisioning: Provide secure internal access via VPN or jump host (as applicable)**
- **Authorization: Approve the internal scope in writing, including IP ranges and sensitive systems to avoid**
- **Third-Party Authorization: Customer is responsible for confirming and obtaining any required approvals from cloud service providers, hosting providers, managed service providers, or other third-party infrastructure owners before internal penetration testing is performed. This includes environments accessed via VPNs, jump hosts, virtual desktops, or shared network infrastructure.**
- **Monitoring: Inform security and network teams about expected testing behavior**
- **Availability: Assign a technical point of contact for coordination and escalation**
- **Remediation: Take action on identified issues post-assessment**

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:** Agreed upon after quote acceptance and completed ROE
- **Testing Window:** Dependent on quantity of IPs
- **Report Delivery:** Within 14 business days of test completion
- **Completion:** Customer sign-off via DocuSign upon full delivery of services

---

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

- www.redesign-group.com/legal

ONSITE SERVICES WILL NOT BEGIN UNTIL THE FOLLOWING PREREQUISITES ARE MET

- A signed quote referencing SKU: SEC-PENINT
- A completed and signed Rules of Engagement (ROE) document
- Verified list of authorized in-scope IP addresses or network segments

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

redesign

The *future* belongs
to the *curious*.

↗ redesign-group.com