PENETRATION TESTING

The Penetration Testing Sourcing Guide

Everything you need to plan, scope, and buy a penetration test that reduces real risk and stands up to scrutiny.

> Written by practitioners who run the tests. Use it to compare providers, understand cost, and ask the right questions before you sign.

20	6	8	100%
QUESTIONS TO ASK	METHODOLOGIES MAPPED	COST FACTORS	MANUAL-LED TESTING

WHY IT MATTERS

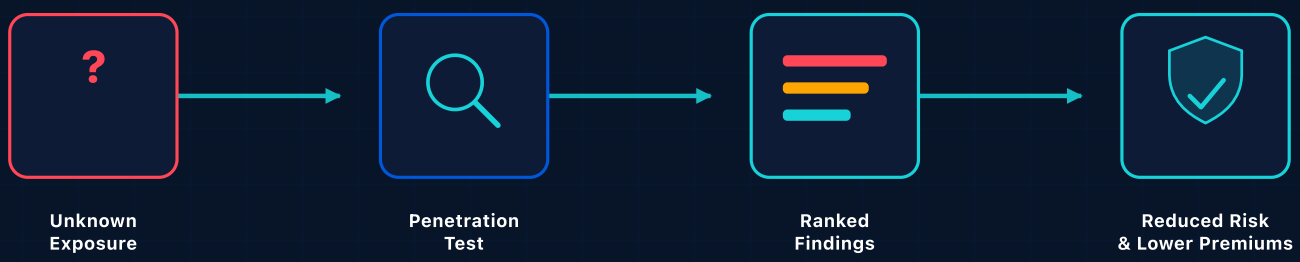
A Pen Test Is a Business Decision

A vulnerability scanner tells you what might be wrong. A penetration test proves what an attacker can do with it and gives leadership the evidence to act.

A well-run engagement delivers:

Validated, real-world risk	Compliance evidence	Lower insurance premiums	Prioritized remediation
Detection & response test	Customer trust	Budget justification	Vendor due diligence

The value is not the list of bugs. It is turning unknown exposure into a ranked, fixable plan your team can execute.



EVIDENCE YOU CAN TAKE TO THE BOARD, AUDITORS, AND INSURERS

> *"Cyber insurers increasingly require proof of regular penetration testing and price premiums on it. A credible report gives you leverage at renewal and real evidence for auditors."*
>
> SUZU LABS · OFFENSIVE SECURITY

STANDARDS & METHODOLOGIES

The Frameworks Behind a Real Test

Credible providers test against recognized methodologies rather than an ad-hoc checklist. Ask which of these guides the engagement, and how.

PTES

Penetration Testing Execution Standard, covering every phase of a professional engagement.

- Scoping through post-exploitation
- Common baseline across vendors

OWASP

WSTG and MASTG define rigorous coverage for web and mobile application testing.

- Injection, auth, access control
- App-layer logic and API abuse

NIST SP 800-115

The U.S. technical guide to security testing and assessment. Common in regulated sectors.

- Planning, discovery, attack, reporting
- Maps to NIST CSF and 800-53

OSSTMM

Open Source Security Testing Methodology Manual, a measurable and repeatable approach.

- Operational security metrics
- Beyond networks: people, process

MITRE ATT&CK

Maps findings to real adversary tactics and techniques so risk is expressed in attacker terms.

- TTP-based attack narratives
- Aligns testing with threat intel

PCI DSS & ISO 27001

Compliance regimes that mandate testing on a set cadence with specific scope requirements.

- PCI: annual + after major change
- Feeds SOC 2 and ISO evidence

THE ENGAGEMENT LIFECYCLE

What Sourcing a Test Involves

A quality engagement has four connected phases. Understand each before you compare quotes, because the gaps between vendors usually hide in scoping and retesting.

PHASE 1

Scoping & Rules of Engagement

Define targets, objectives, test type (black / grey / white box), timing, and safety limits. Scope drives both cost and value, so get it in writing before anything else.

FIXED SCOPE IN WRITING

PHASE 2

Testing & Exploitation

Hands-on testers perform recon, find and chain vulnerabilities, and safely demonstrate real impact. Automated tooling supports the work but never replaces manual testing.

MANUAL-LED

PHASE 3

Reporting & Debrief

You receive a ranked report with reproducible evidence, business impact, and clear remediation, plus a live walkthrough for both technical teams and executives.

EXEC + TECHNICAL

PHASE 4

Remediation & Retesting

After you fix issues, testers verify the fixes hold and issue an updated report. Confirm whether retesting is included before you compare prices.

VERIFY THE FIX

CHOOSING A PROVIDER

What Separates a Test From a Scan

Six things to evaluate, with the question that cuts to the truth for each. These are the differences quotes rarely make obvious.

Tester Talent

CERTS
OSCP / CREST

The people matter more than the brand. Know who runs your test and what they have done before.

ASK
"Who performs the testing, and what are their certifications and experience?"

Methodology

DEPTH
MANUAL-LED

A relabeled vulnerability scan is not a pen test. Confirm real, hands-on exploitation against a standard.

ASK
"Is this manual testing to PTES/OWASP, or an automated scan with a report?"

Scope & Cost

PRICING
RIGHT-SIZED

Cost is driven by scope size, complexity, test type, and timing, rather than a flat sticker price.

ASK
"How is scope defined and priced, and what changes the cost up or down?"

Reporting

OUTPUT
ACTIONABLE

You live with the report long after testing ends. It needs ranked findings, evidence, business impact, and fix guidance.

ASK
"Can I see a sample report, and does it include an executive summary?"

Retest & Support

AFTER
INCLUDED?

A finding is not closed until a retest proves the fix works. Confirm it is in scope, not an upsell.

ASK
"Is remediation retesting included, and for how long after delivery?"

Delivery Model

CADENCE
POINT VS PTAAS

A point-in-time test is a snapshot. PTaaS adds continuous testing and a live results portal.

ASK
"Do you offer point-in-time, PTaaS, or both, and which fits my risk?"

The cheapest scan is rarely the best test.
Buy expertise, evidence, and follow-through, not a bare PDF.

NEXT STEP

Scope Your Next Pen Test With Confidence

You now have the framework to compare providers on what matters.

Bring us your environment and objectives. We will help you right-size scope, map it to the appropriate methodology, and give you a fixed quote, with no pressure and no jargon.

Tests run by the same practitioners who write this guide.
Manual-led testing, evidence-backed reports, retesting included.

SOURCING CHECKLIST

- ✓ Who performs the testing, and their certs?
- ✓ Manual testing or an automated scan?
- ✓ Which methodology guides the work?
- ✓ How is scope defined and priced?
- ✓ What does the report include?
- ✓ Is remediation retesting included?
- ✓ Point-in-time or continuous (PTaaS)?

ABOUT SUZU LABS

Suzu Labs is a cybersecurity firm run by practitioners: red teamers, offensive security operators, and threat intelligence analysts. The team that scopes your test is the team that runs it, and stays through remediation.

WHAT ELSE WE DO

- → Penetration testing & CAO
- → Red teaming & adversary simulation
- → Incident response & forensics
- → Dark web monitoring
- → AI security advisory
- → Governance, risk & compliance

Suzu Labs

OFFENSIVE SECURITY · THREAT INTELLIGENCE · AI SECURITY · SUZULABS.COM