2025

# Penetration Testing BUYERS GUIDE

SENCODE LTD

# INTRODUCTION

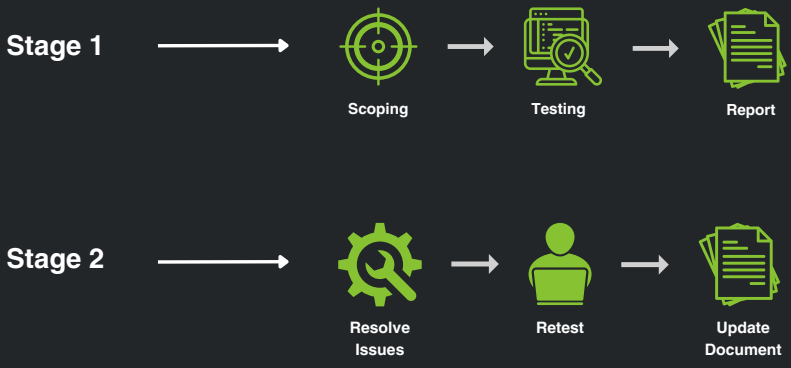
This guide will walk you through the fundamentals of penetration testing, what to look for in a prospective partner, and how much you can expect to invest. By the end, you will feel well-equipped to make an informed decision about your cyber security needs.

### What is Penetration Testing?

Penetration testing is a controlled simulation of cyber attacks on your systems. By revealing vulnerabilities before malicious actors do, pen testing helps you prevent data breaches, system outages, and reputational damage. Common penetration testing services include:

- **Web Application Penetration Testing** (Against a web application, https://myreallygreatwebapp.co.uk)
- **API Penetration Testing** (https://api.myreallygreatwebapp.co.uk)
- **Network Penetration Testing**
  - Externally (External IP Ranges, 188.166.170.130 etc)
  - Internally (Internal IP Ranges, 192.168.1.10 etc)
- **Cloud Penetration Testing** (Hosted in GCP, Azure, AWS)
- **Mobile Application Penetration Testing** (Android of IoS Mobile Apps)
- **Social Engineering Assessments** (Your Human Beings)

## Typical Penetration Testing Staged Process




Links are underlined

# UNDERSTANDING PENETRATION TESTING COSTS

There are many elements to consider when choosing a supplier. Below you will find a defined list of areas you should consider before selecting the vendor.

**Pen testing prices are usually based on:**

- **Scope & Complexity:** Volume of applications, number of user roles, network segments, or endpoints.
- **Provider's Expertise, Accreditations or Disciplines**: CREST-accredited or highly specialised professionals may charge more.
- **Testing Perspective**: Black box, grey box, or white box approaches can alter the required days.
- **Retesting & Support**: Some vendors include one round of retesting free of charge. Others do not.
- **Bulk Discounts**: Purchasing multiple days or recurring assessments in a single contract can reduce per-day costs.

**Typical Examples**

- A medium-sized web application (50 pages, multiple user roles, moderate complexity) may need 4–6 days at a rate of £1,000 per day, costing around £4,000–£6,000.
- A medium-sized internal network (80 employees, end-user devices, 25 servers, Active Directory, basic segmentation) could require 5–7 days, totalling £5,000–£7,000.

If you want a full breakdown of all the factors that go into costing a penetration test project. Read our in-depth blog post, linked below.

"How much does penetration testing cost? - Blog"

# WHAT CAN INFLUENCE THE COST OF A PENETRATION TEST?

More Assets
More Complexity
More support

=

More Days Required

---

Skills, Certifications & Commercial Experience

=

Typically Higher Day Rate

---

Bulk buying days
Repeat Customer
Large Scope

=

Discounted Price

# KEY FACTORS INFLUENCING SERVICE SCOPE AND COST

## WEB APPLICATIONS

### Complexity
- Data inputs
- Unique pages

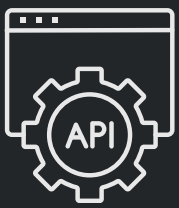
### User-roles
- Standard
- Admin
- Super Admin

### API Endpoints
- Endpoint volume
- Endpoint complexity

## API

### Complexity
- CRUD Operations (Volume of endpoints)

### User-roles
- Standard
- Admin
- Super Admin




### Documention
- Swagger
- Postman
- OpenAPI

# SERVICE DATA FACTORS THAT INFLUENCE THE SCOPE AND PRICE

## NETWORK PENETRATION TESTING

### Wireless Networks
Wi-Fi

### Active Directory
Presence of AD

### Complexity
Segmentation
Device Volume
Virtualisation
Authentication
Perspective

## Mobile App Penetration Testing

### Platform
Android (APK)
iOS (IPA)

### User-roles
Standard
Admin
Super Admin

### Complexity
Data Input
Code
SDK's
Authentication
API Endpoints

# PENETRATION TESTING APPROACHES AND COMPLIANCE

**Conventional Penetration Testing**

- Wide-ranging assessment searching for as many vulnerabilities as possible.
- Particularly useful for regular check-ups of overall security posture.

**Objective-Focused (Goal-Based) Testing**

- Targets a specific outcome, like accessing sensitive data or disabling a business-critical system.
- Can be quicker and more narrowly scoped, simulating a determined attacker's objective.

## Regulatory Compliance in the UK

Many regulations encourage or mandate regular penetration testing. Failure to comply can lead to serious financial penalties and reputational harm. Notable UK regulations include:

**Data Protection Act 2018 (DPA 2018)**

National implementation of GDPR principles, imposing strict controls on handling personal data.

**General Data Protection Regulation (GDPR)**

Still applies in the UK. Strong emphasis on privacy and data breach prevention.

**Digital Technology Assessment Criteria (DTAC)**

Framework used by the NHS for assessing digital healthcare solutions.

**Payment Card Industry Data Security Standard (PCI DSS)**

Mandatory if you store, process, or transmit payment card information.

# TOP CONSIDERATIONS WHEN SELECTING A PEN TESTING PROVIDER

There are many elements to consider when choosing a supplier. Below you will find a defined list of areas you should consider before selecting the vendor.

**Expertise & Accreditations**

- Look for testers with recognised certifications (CREST, OSCP, CISSP).
- Check if the company itself is CREST-accredited.
- Confirm that you can request a specific consultant's credentials if required.

**Sample Reports**

- Does the report explain issues for non-technical readers?
- Is it detailed enough to offer clear remediation steps rather than surface-level findings?

**Tailored Testing & Thorough Scoping**

- Ensure they customise each project to your particular environment.
- Expect questions about assets, user roles, test perspectives (black, grey, or white box), and deadlines.
- Proper scoping avoids scope creep and sets clear expectations.

**Effective Communication**

- Reliable firms provide regular status updates and instant alerts for critical vulnerabilities.
- Open communication channels are crucial for a smooth assessment.

**Reporting & Support**

- A thorough final report should include actionable next steps.
- Check whether remediation help and retesting (often chargeable) are included.

**Reputation & Experience**

- Seek client testimonials, case studies, or references.
- Extensive experience in complex projects is often a plus.

**Ethical & Legal Compliance**

- Request NDAs and confirm data privacy measures.
- Ask about their approach to meeting legal and regulatory obligations.

**Costs**

- Expect daily rates between £900 and £1,700, depending on scope and complexity.
- Insist on a breakdown of fees (including retesting).
- Balance quality with budget—cheapest is not always safest.

Links are underlined

Get in touch today for a free, no-obligation quote

# VENDOR ASSESSMENT

A penetration test is not merely a box-ticking exercise for compliance. You are trusting a partner with your sensitive systems, data, and people. Opting for the cheapest, least-qualified provider can lead to inadequate scoping, superficial reports, and missed critical vulnerabilities. Assess each vendor and make your own decision regarding suitability.

**Certifications**

**Example Reports**

**Scoping Quality**

**Communication**

**Reputation**

**Cost**

**Vendor Assessment Checklist**

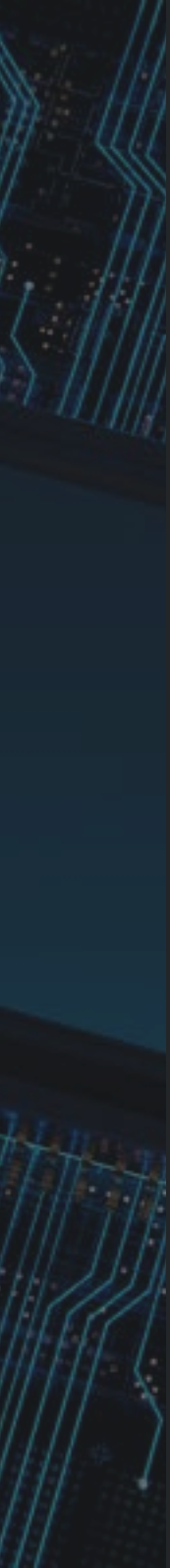
- [□] CREST accredited?
- [□] Certified testers? (OSCP, CISSP, CREST CRT, etc.)
- [□] Thorough scoping during the initial scope? (assets, user roles, test perspective)
- [□] Clear communication offered? (regular updates, quick alerts)
- [□] Can a sample report be provided?
- [□] Comprehensive reporting? (Assess the sample report, remediation steps, guidance)
- [□] References? (track record of success)
- [□] Data privacy & NDAs? (legal/ethical compliance)
- [□] Transparent costs? (itemised quotes, potential retest fees)
- [□] Ongoing support? (remediation help)
- [□] Free retesting? (free or paid retesting)

Links are underlined

Get in touch today for a free, no-obligation quote

# VENDOR ASSESSMENT TABLE

| Checklist Item | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| Vendor Name | | | | |
| CREST accredited? | | | | |
| Certified testers? (OSCP, CISSP, CREST CRT, etc.) | | | | |
| Thorough scoping (assets, user roles) | | | | |
| Clear communication (regular updates, alerts) | | | | |
| Sample report provided? | | | | |
| Comprehensive reporting (remediation guidance) | | | | |
| References? | | | | |
| Data privacy & NDAs (legal/ethical compliance) | | | | |
| Transparent costs (itemised quotes, retest fees) | | | | |
| Ongoing support (remediation help) | | | | |
| Free retesting offered? | | | | |



# CONCLUSION

Selecting the right penetration testing provider can save your organisation from costly data breaches, reputational damage, and non-compliance fines. Considering these factors, from CREST accreditation to scope clarity, expertise, and post-engagement support, ensures you invest wisely in your cyber security.

A successful pen test is more than a technical exercise—it is a strategic partnership that helps you stay a step ahead of ever-evolving cyber threats. By prioritising quality and thoroughness, you can protect what matters most: your data, your operations, and your clients' trust.

**Ready to Secure Your Systems?**

At Sencode, we are committed to delivering top-tier, CREST-accredited penetration testing tailored to your unique needs. Whether you need a comprehensive audit or a targeted, goal-based test, our experienced consultants are here to help.

Get in touch today for a free, no-obligation quote and let's take the first step towards securing environment—together.

Links are underlined