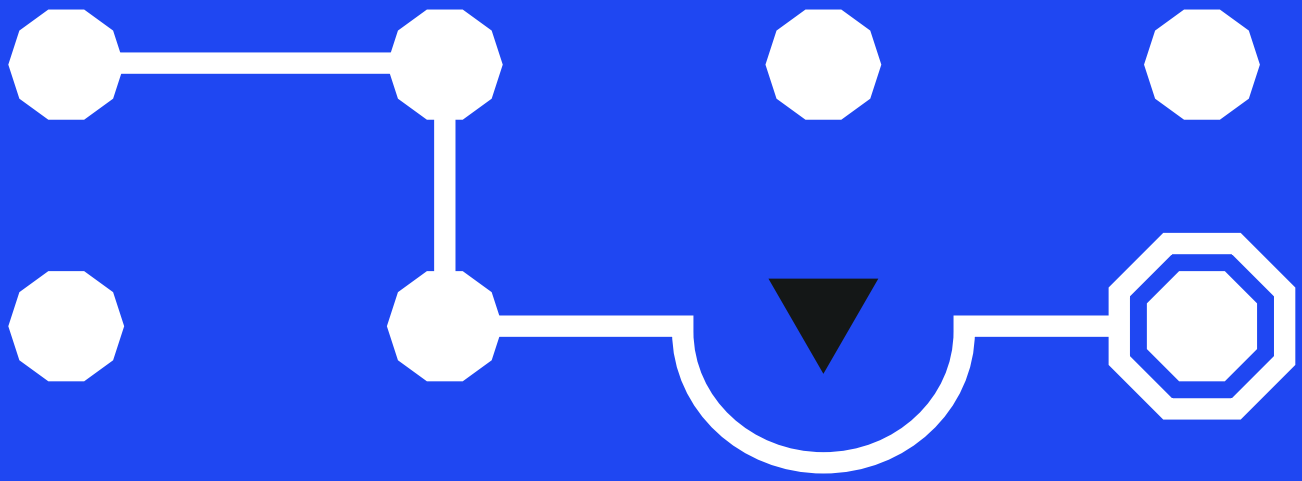
How to select a credible Penetration Testing Vendor



Navigating the Minefield.

Plotting this journey can be fraught with false dawns, but we hope that the next few pages will help you select a clear path to selecting the right testing partner.

The depth of evaluation needed to select the right vendor will be partially determined by whether the requirement is for a single instance of a penetration test or a more regular test programme.

As a starting point it is useful to understand what constitutes accepted best practice in the penetration testing industry. Typically, mature organisations, including Tier 1 banks, will insist on the CREST (Council of Registered Ethical Security Testers) accreditation as a minimum standard for the vendors on their testing panels.

Incidentally, CREST provides a handy guide for procurement teams, which can be freely downloaded from the website:

Penetration Testing Services Procurement Guide

See Pdf

In summary, CREST recommends that the following points are considered when selecting a vendor:

As with any business you should consider if the company has a solid reputation, history and ethics.

Are they delivering high quality, value for money services?

Check for strong accreditation. It is a minimum pre-requisite for the most mature mature buyers, as it lowers their risk.

CREST

Can they evidence a dynamic R&D capability?

Do they themselves practice effective security and risk management.

Does the team comprise highly competent, technical testers?

This provides a good framework for penetration testing delivery, but may not be the panacea that qualifies out the unsuitable candidates. It should influence the process, but let's take a look at the other factors that customer feedback suggests should be in the mix.

1. Independent Specialist

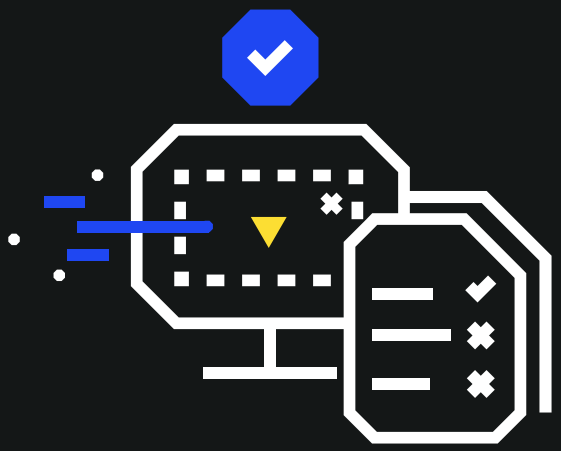
Some may be of the opinion that using one company to deliver multiple services could make life slightly easier for the procurement team. However, might ease of purchase prevail at a cost of shortcomings in the service delivery?

Companies are proud of their relative strengths in their signature service offerings, but experience tells us that few companies that can be considered best of breed across their entire portfolio?

Bearing in mind that share prices can plummet, reputations can be lost and large fines accrued in the event of a security breach, **can a penetration test just be considered another "tick in the box"?**

We don't think so

- Take time to consider if your preferred vendor is an expert at penetration testing or just offering a half-baked service offering in an already overcrowded portfolio?
- Ultimately, how comfortable do you feel knowing that a vendor is not only "marking your work" but also selling you the solutions?
- Is the report completely impartial; not simply lending itself to opportunities for promoting costly vendors solutions in the remediation plan?



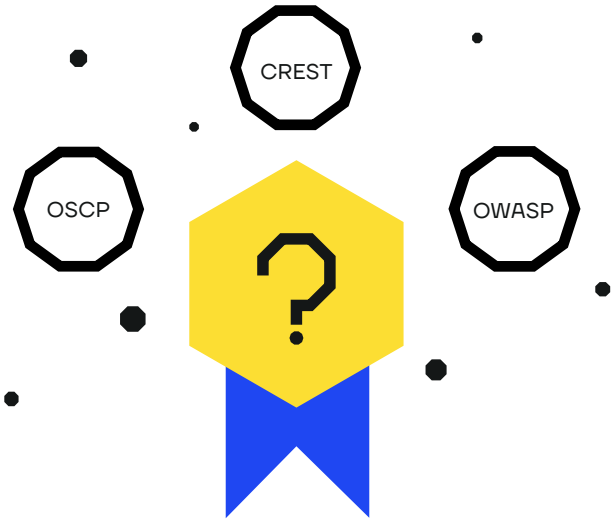
The report is about giving you visibility of security issues, not a thinly veiled shopping list of solutions that promise to 'secure your enterprise'.

2. Technical Excellence

The most security conscious companies take comfort in knowing that their preferred vendor can demonstrate a high level of technical competence, but how do you measure this?

How can you be sure that the allocated tester has the appropriate attitude and skillset to provide you with the visibility that the test is expected to deliver?

The reality is that there is no defined badge of honour, however it would be prudent to ensure that their approach is building on recognised methodologies such as OSCP, CREST and OWASP. It is also good practice to pose a few questions to the vendor to understand if the recruitment and training bar is set high enough for them to be able to deliver to the standard you expect:



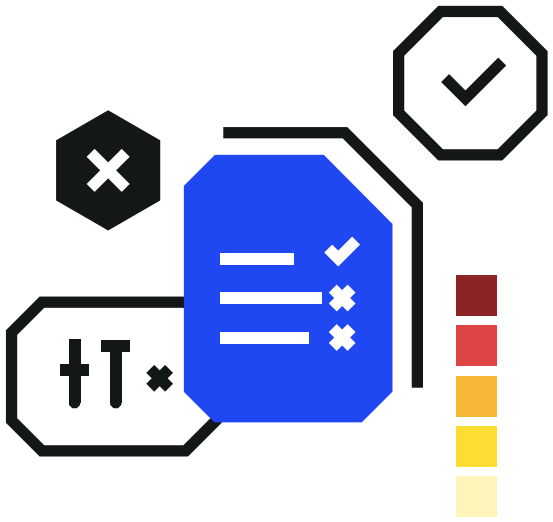
- What level of accreditation does the company hold?
- What technical validation do all new employees go through prior to being offered employment as a security tester?
- How soon will a new tester be deployed on a paid customer engagement from commencement of their employment?
- How do you ensure that their testers are going to keep you ahead of the security curve?

3. Clear, Concise Reporting

The report is the ultimate deliverable, which typically serves as a guiding light in the remediation process or as a valuable business enabler for third party engagement. This places an awesome responsibility on the part of the vendor to make sure it is fit for purpose.

Some reports have been known to simply contain scanning tool output dumped into a hefty document. Many offer no evidence of manual verification of findings or evidential screenshots, putting more strain on the remediation process.

An experienced vendor will provide a tiered report encompassing an executive summary and a full technical breakdown of any issues with appropriate remediation advice.
An experienced vendor will provide a tiered report encompassing an executive summary and a full technical breakdown of any issues with appropriate remediation advice. Innovative vendors may also be able to offer creative reporting solutions that could really help in expediting the remediation process.



So, keep it simple

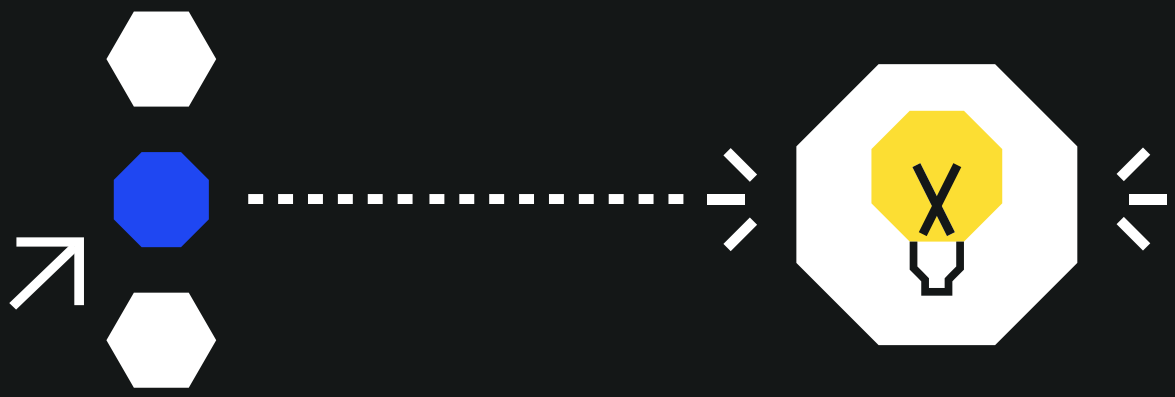
- Ask the vendor for a sample test report.
- Explore innovative reporting solutions offered by the vendor that may provide additional value.

4. Appropriate Scoping

Armed with the best methodologies, highly accredited testers, and great reporting, is this enough credibility to enable you to make an informed decision?

For some maybe, but those in the know often need a little more to sign on the dotted line:

- Has the vendor taken the time to identify your pain point and propose a unique solution; or has it simply been a question of “Here are our service pillars – which one is best aligned to your requirement?”



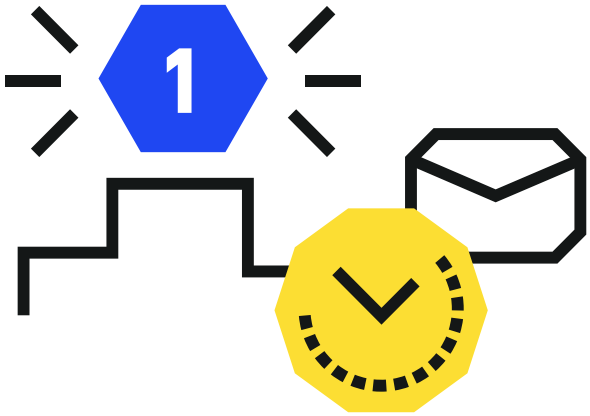
- How can you be sure that the proposal has not simply been hastily penned by an over-zealous salesperson with £££ signs in their eyes?

A great proposal will go through a technical QA process and for more complex projects you should expect some technical representation at scope inception – look for a thorough document control process in the proposal that reflects technical input as part of the sign off process.

5. Responsiveness

Ever felt at the behest of your penetration testing vendor when it comes to waiting for a proposal?

Many of your peers express frustration at playing the waiting game. How do you feel when you are offering someone your business, but you don't feel like you are their priority? In a burgeoning and competitive marketplace and with the world at your feet, don't you deserve a proposal in a timely manner?



Some may think so.

- Does the vendor really want your business and is that reflected in the speed and comprehensiveness of their response times and deliverables?
- How confident are you that the lines of communication will be open with the account manager and technical team pre, during and post testing?
- How long will you have to wait to find out about a business critical vulnerability?
- How easy would it be to be to set up a scoping or wash with the vendors on your radar?

secforce.com