bugcrowd

Penetration Testing

THE PROS & CONS OF FOUR COMMON METHODS

When it comes to facing a difficult choice, pretty much all of us can relate to the feeling of ripping a fresh sheet of paper out of your notebook, drawing a line down the middle, and starting a pros and cons list.

Today we're looking at the pros and cons of different penetration testing methods. While there are a number of different penetration testing methodologies that vary by target type, compliance initiative, and more, there are four primary methods for deploying services generally. These penetration testing methods are traditional, crowdsourced, internal, and a mixed approach.

COMPARE METHODS NOW

1 TRADITIONAL PENETRATION TESTING

Many organizations still rely on traditional penetration testing services, often as a result of budgetary or procurement constraints. The 'traditional' model comprises one or two testers working against a set methodology for a defined period, usually anywhere from three days to two weeks. This format is a mainstay of the security industry, and executives and business leaders are pre-sold on the need for it.

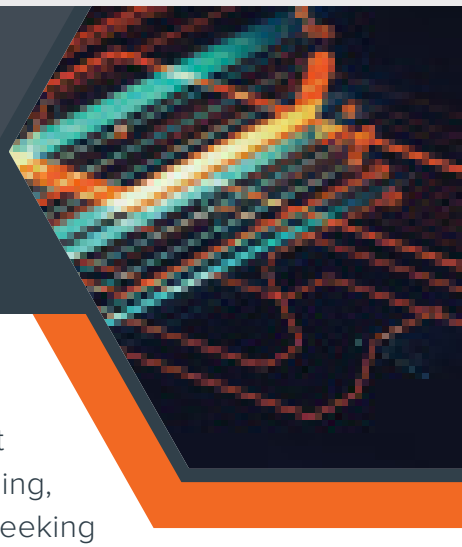
PROS

- Established budget line item
- A known quantity
- Best suited to targets that require physical presence to access/test

CONS

- Delays to scheduling and results
- Inflexible with questionable skill fit
- Not optimized to incentivize true risk reduction

2 CROWDSOURCED SECURITY PENETRATION TESTING



The crowdsourced penetration test is a comparatively new method of testing. Crowdsourced options utilize a large pool of remote, pay-per-project testers. Often combined with an incentivized 'pay for results' approach to billing, crowdsourced testing is quickly becoming the top choice for organizations seeking more from their security testing services.

PROS

- Rapid setup and time to value
- Real-time results and SDLC integration
- Option to 'pay for results' instead of time

CONS

- Not optimized for highly sensitive or physical targets too big to ship
- 'Bounty' approach may not fit buying cycles
- New business case may be required

3 INTERNAL SECURITY TESTING

While often not feasible for smaller organizations, some enterprises prefer to build and maintain in-house teams of security testers. This approach allows the organization to set its own testing schedule, and may reduce barriers in some areas, e.g., provision of credentials.

PROS

- Best for extremely sensitive work (e.g., Secret, NOFORN)
- Tests can be run as frequently as needed
- Little marginal cost to testing

CONS

- Labor-intensive to set up and maintain
- Impossible to retain all possible testing skills
- Hard to acquire new skills when needed

4 A MIXED TESTING APPROACH

Some organizations use a combination of traditional, crowdsourced, and internal testing to meet the specific needs of each project.

PROS

- Includes the best aspects of each method
- Potential for thorough security coverage
- Testing depth is as-needed for each project

CONS

- Includes the worst aspects of each method
- Complex to arrange and maintain
- (Potentially) extremely high-cost

Now that you have an overview, here's a little data to help you make the best decision. In a recent survey, respondents placed traditional penetration testing neck-and-neck with crowdsourced testing on total cost. However, since crowdsourced delivers more, higher-quality results, it's a clear winner for ROI. Crowd-powered penetration tests identify on average 7X more high-priority vulnerabilities than traditional penetration tests. It's no wonder that crowdsourced penetration testing is gaining traction with organizations of all sizes. They now account for between 20-30% of all security testing, depending on organization size.

By drawing on an elastic, fully managed network of premium testing talent, crowdsourced security platforms offer organizations a faster path to compliance without sacrificing the critical insights that help keep products and customers safe. **Contact Bugcrowd to launch your first penetration test and begin harnessing the power of the Crowd.**