Penetration testing challenges

BY ANNA HAMMOND · NOVEMBER 3, 2022 · LAST UPDATED ON MARCH 6, 2025

How best can businesses navigate the common penetration testing challenges that arise when improving their security posture? In one of our last blogs, we discussed how Pentesting as a Service updated the pentesting format. As a rendition of Software as a Service, this change led pentesting to be more cost efficient, scalable and ultimately more adjustable depending on the needs of a business.

Despite the sleeker method of delivery that this brought however, businesses continue to incur issues when setting up penetration testing. In this blog, we will explore the origins and solutions of the most typical penetration testing challenges that businesses face. With the global penetration testing market size expecting to grow from $1.6 billion in 2021 to $3.0 billion by 2026 (a Compound Annual Growth Rate of 13.8%), removing the barriers to their most effective use will be paramount to improving global security.

When do you need a penetration test?

Before diving into the challenges of penetration testing, it's perhaps necessary to note the exact role that penetration testing has. With so many kinds of security solution on the market, it's important to first dispel a cybersecurity myth: bug bounty providers compete with pentesting. Bug bounties and penetration tests cater to *different* needs, both playing a key role in overall security maturity. It's far more accurate to say they complement each other, providing advantages in separate areas. Sándor Incze, CISO of CM.com described bug bounty as the 'cherry on top' of their security infrastructure. Essentially, it should be thought of as one part of the many layers that make a great cake/security system!

There are several reasons why a company may opt for Pentesting as a Service as opposed to a bug bounty program.

It may be relatively early days regarding your security journey with a product or platform that hasn't gone through much testing, meaning there are likely to be many vulnerabilities. In this case, a full-blown public bug bounty would simply be overwhelming, whereas a penetration test may allow you to first take care of the 'low hanging fruit'.

Perhaps you're looking to simply get a glimpse of the current security posture for a new asset. This can be extremely useful in determining the scope of future testing and indicating your current maturity.

For some, there is a requirement to fulfill particular security compliance, which often comes with a dedicated deadline. The test, therefore, needs to be a verifiable demonstration of your compliance.

Key penetration testing challenges

But even with the benefits that PTaaS has brought to pentesting, companies often experience difficulties when optimising their tests. Diving right in, here are some of the most common challenges.

1. Continuously changing environments

Being 'agile' in modern software development has been a tenant of the industry in recent years. Being able to respond rapidly to changes in the market and providing fast updates to your product, however, leads to issues in security. Fast release cycles are difficult to keep up with regarding penetration tests, as they must revised and rerun quickly as fast. Assessing your true posture and risk in these changing environments becomes a challenge.

2. Rapid growth

Unsurprisingly, an expanding business often means an expanding attack surface. Adjusting pentests accordingly can almost feel like building the plane while it's already in flight. According to Help Systems, 42% of respondents conduct pentests only once or twice per year. This is highly indicative of a lack of retesting and severely less visibility than needed.

3. Cybersecurity skills shortages

Within small internal security teams, knowledge of the latest techniques used by attackers is often scarce. When this is the case, pentests often reflect this lack of expertise and don't provide an accurate picture of the overall security. For some organizations, there is also an issue of trust when relying on a smaller subset of researchers. When working with limited knowledge bases and skillsets, you become unaware of hidden risks.

4. Cyber threats are evolving

Even with more frequent pentesting, the rate that cybersecurity attack methods evolve pose significant difficulties for businesses. To maintain the knowledge needed internally is often insurmountable.

How can PTaaS address these pentesting challenges?

PTaaS platforms can differentiate themselves to deliver real value by addressing pentesting challenges head-on.

Intigriti's Hybrid Pentesting is a simple and cost-effective method of PTaaS that utilizes the unique expertise of hacking communities. By introducing the bug bounty approach to pentesting, you gain a greater focus on impact due to researchers being motivated to find high-impact vulnerabilities.

Pay for impact

Rather than wasting money on lengthy set processes, with Hybrid Pentests, you only pay for results. With the severity of vulnerabilities tied to the payout, hackers are motivated, and the impact for you is maximized.

Short lead time and simplified workflows

Start a security test with a lead time of typically 2-3 weeks. Our streamlined platform enables both fast setup and full vulnerability management.

Dynamic and fully adjustable test coverage

It's completely up to you how researchers carry out the pentest. They can follow the desired methodology of your choosing or explore freely using their creative flow.

Find the exact skills relating to your project requirements

Hybrid Pentesting allows you to access the unmatched skill pool of our ethical hacking community. Researchers can be handpicked for their knowledge bases such that you have maximum impact on your project.

Streamlined communication and result transparency

You can communicate with the chosen researchers directly through our platform. All progress and results are displayed live.

In short, Hybrid Pentesting addresses the shortcomings of traditional pentests. By tapping into the skill base of hacking communities, speed and impact are prioritized.

Want to know more about setting up and launching Hybrid Pentesting?

Intigriti is the leading European-based platform for all-in-one solutions for security, providing both PTaaS and bug bounty programs.

The platform enables organizations to reduce the risk of a cyberattack by allowing Intigriti's network of security researchers to test their digital assets for vulnerabilities continuously. To find out more about Hybrid Pentesting, contact our team today!

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com