Key terms in crowdsourced security

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

Do you know your bug bounty from your Hybrid Pentest?

Cybersecurity moves fast. And if keeping up with the latest emerging threats wasn't enough, knowing the best way to defend against them can feel just as complicated.

When it comes to crowdsourced security, we've come a long way since the days of there only being internally managed bug bounties. Recently, Intigriti released Hybrid Pentesting, our take on what's become known as Pentesting as a Service, representing just one of the many different services we now provide.

But what differentiates them all? Which one is right for your business?

In this blog, we'll go on a pitstop tour through crowdsourced security to help you understand each service, its features, and when it's best applied. By the end of it, you will be a crowdsourced cybersecurity expert!

What is a Vulnerability Disclosure Policy (VDP)?

A VDP is a way of enabling businesses to mitigate security risks by providing support for the coordinated disclosure and remediation of vulnerabilities before they're exploited by cybercriminals. VDPs tend to give guidance on how the vulnerabilities should be reported and any other 'rules of engagement'.

So why would an organization bother with a bug bounty when they could just set up a VDP? The main issue with self-hosting a VDP is that it places a drain on your resources. The process of managing incoming reports, triaging any issues, and, of course, fixing them is left entirely with your internal security team, who are often overworked as it is. This is particularly problematic when you can't guarantee the quality of any incoming reports, as huge amounts of time can be wasted going through low-quality submissions.

VDPs can also struggle with the nature of the submission method. Often an email can go unnoticed in an inbox compared to the complete visibility offered by a bounty platform. VDP is, however, the essential idea at the heart of bug bounties, although bug bounty platforms take it to the next level.

The benefits of VDP through bug bounty platforms

VDP is essentially a 'see something, say something' approach. While it allows researchers to test your security, it doesn't incentivize hackers to continuously test a business. In our Ethical Hacking Insights 2022 Report, we found that 26% of ethical hackers would not work with companies outside of a bug bounty platform, and 23% said they would prefer not to.

Managing and nurturing a community has other benefits as well, as you can find the hackers with the exact skills needed to test your business most effectively. This can be particularly useful when you're looking for a more controlled testing environment that's similar to a traditional penetration test.

Additionally, when hosting your program through a bug bounty platform, you gain the key benefit of a triage team that acts as a go-between, taking the pressure off internal security teams.

Private vs. public bug bounties

A publicly-listed bug bounty program is open to any would-be ethical hacker. These programs tend to focus on testing assets that have a high level of security maturity, as they are open to so many researchers.

A private bug bounty program, on the other hand, allows businesses to tap into researchers with particular skillsets, based on your requirements. These programs are only visible to those invited, but additional researchers can be added as necessary.

When new to crowdsourced security, organizations generally start with a private program before eventually moving to a full public program. It's crucial to note, however, that regardless of private or public, every program can be constructed with a specific scope, budget limitations, and bounty schemes.

What is Pentesting and Pentesting as a Service?

Penetration testing is a controlled, time-boxed simulation of an attack against a system or network. It should be noted that bug bounties are not intended to be a replacement for traditional pentesting, but rather they cater to separate needs. Pentests can be thought of as a step before private bug bounties, where the scope is often even more specific, such as checking the robustness or compliance of a new feature.

The key difference with a pentest is the time-boxed approach. This is where Pentesting as a Service (PTaaS) has stepped in, by modernizing and improving the traditional format. PTaaS delivers pentests through a centrally-hosted portal and with real-time updates, taking care of backend overheads to deliver a more scalable and cost-efficient solution.

We wrote a handy blog explaining PTaaS to help you understand.

Intigriti's Hybrid Pentesting

Hybrid Pentesting is the name of Intigriti's PTaaS offering. It's the traditional approach of a pentest, except you get access to the wealth of skills in our hacking community to get the best job done.

You can start a test with a lead time of just two or three weeks, through a simple-to-use platform, where you only pay if results are found.

Hybrid Pentesting is designed to meet separate needs from that of bug bounties. One, it can provide a proof of test that can be used to prove your compliance. Secondly, Hybrid Pentests can be carried out in a short window, supporting businesses that are under time pressure.

Finally, hybrid pentests can use specific methodologies compared to the ‘free form’ of bug bounties, once again useful if you’re needing to prove your posture against something like OSSTMM.

Live hacking events

Live hacking event are intense hacking periods in which some of the most skilled hackers come together to collaboratively test. By sharing ideas and attack strategies, these events can produce a high volume of reports in a short time period, while also providing a fun event demonstrating a businesses commitment to their security. More information on live hacking events can be found in this handy blog.

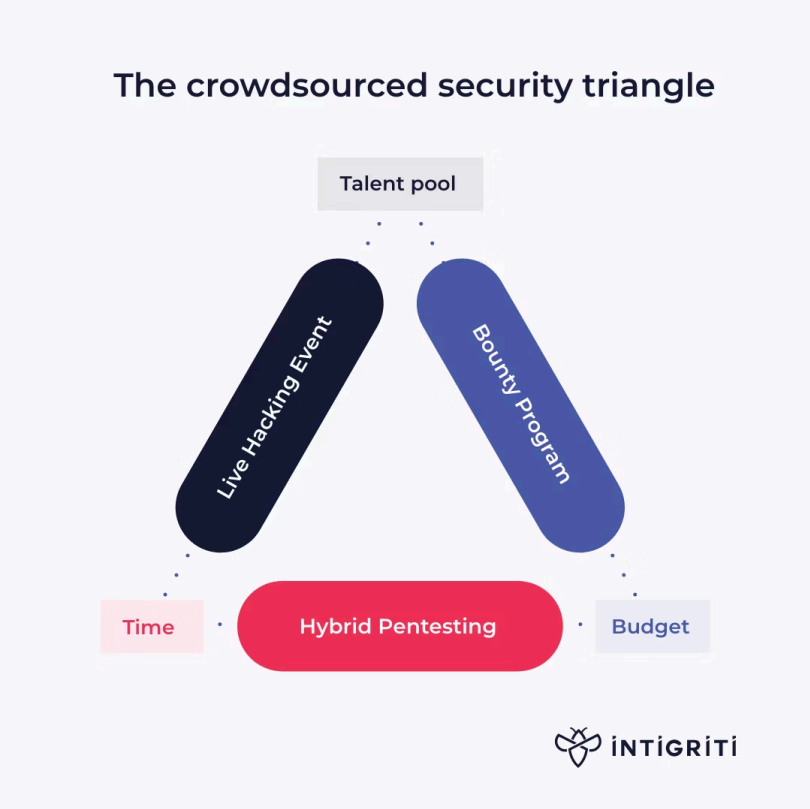
The Crowdsourced Security Triangle

So, how do we consolidate these various security solutions? Which one is for my business? To help you better understand how these solutions interplay, let us introduce you to the Crowdsourced Security Triangle.

When choosing any crowdsourced security solution, three key factors are at play: the **talent pool**, the **time available,** and the **budget**. When looking at crowdsourced security, businesses are driven to their most appropriate solution based on gravitation to two of these factors.

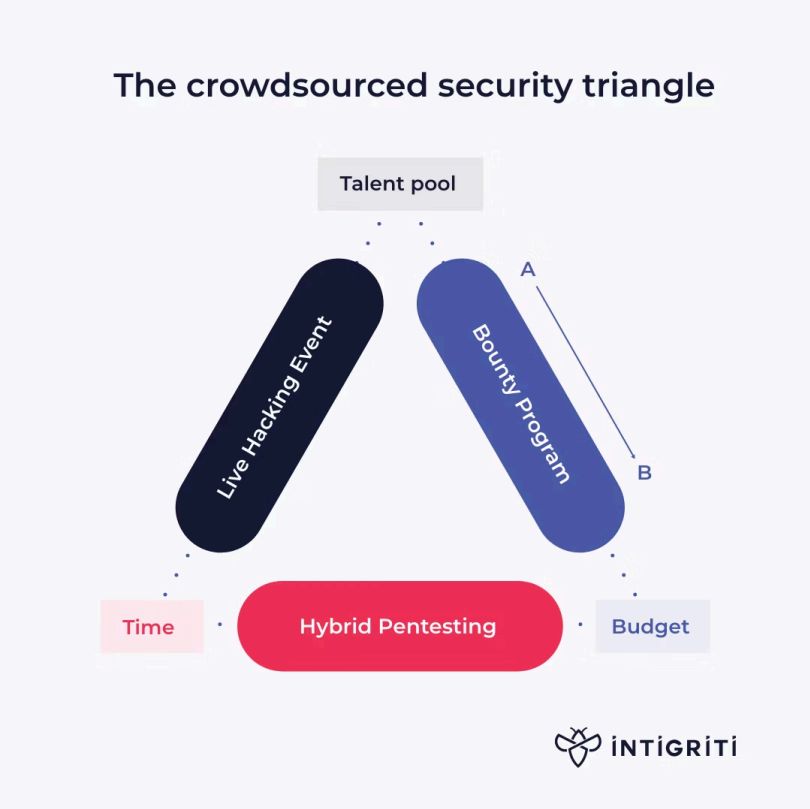
For example, say you need to test some specific new features of your product, but you need to deliver the security result on a tight timeframe and small budget. In this scenario, a Hybrid Pentest would be the most appropriate.

The factor that is absent in this example is, of course, the talent pool. If you want to get fast testing on a budget, it might not be possible to capture the attention of lots of hackers. However, in scenarios such as this, the tight scope often involves a specific methodology (such as OSSTMM), which can be easily conveyed to the small number of hackers used.



To take a different example, imagine you want to test a mature asset to ensure it is 100% resistant to any creative penetration technique out there. Depending on your budget, this would fall into going with a bounty program or a live hacking event. Hacking events are intensive and can deliver a large number of reports quickly, but they're costly. Bounty programs are less costly, but they take a longer period of time to obtain the reports.

In this way, each solution is primed to fill the limitations that are placed on security teams. However, it's crucial to note there are not simply three positions in the triangle. Every business has different budgets, time frames and required scopes, so even if you've say settled on a bug bounty as your solution, it can be bespoke to these factors. Maybe you have a greater budget, and more desire to access the whole talent pool – your position in the triangle might be A. Whereas those with a smaller budget and smaller scope might be at position B.



Between Hybrid Pentesting, bug bounties and live hacking events, there are crowdsourced security services that can cater to every need and level of security maturity. Hopefully this blog helped you understand which crowdsourced solution is right for you. And our help doesn't end there! If you decide to go for a bug bounty, we've also got a free-to-use bug bounty calculator that helps you calculate the appropriate bounty to use.

When you go with Intigriti, you get access to all of these services whilst also gaining the benefits of our industry leading community management.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com