DARKHORSE

How To Decide When Deciding

Fractional Pentesting vs. Bug Bounty vs. Vulnerability Disclosure vs. Penetration Testing

<u>Free</u> VDPs & Bug Bounties

Over 50% of all VDPs get fewer than 25 reports annually. DarkHorse offers free VDPs & bug bounty programs - with no restrictions - for any organization with 25 reports per year (measured on a quarterly basis).

>50%
of organizations are eligible for a free VDP

~20%
Of organizations are eligible for a free bug bounty

About DarkHorse

Having spent over a decade in crowdsourced and application security, and seeing the immense amount of value that VDPs, bounties, and pentesting can provide organizations, DarkHorse is on a mission to make crowdsourced and offensive security accessible and affordable for everyone.

Book a meeting with DarkHorse: darkhorse.sh/meeting

DARKHORSE's Perspective

- **Every org should have:**
  - VDP. And with DarkHorse offering VDPs for free, there's no reason for any org *not* to have one.
- **For maximum risk reduction:**
  - Bug bounty. Nothing is better at identifying vulnerabilities at scale.
- **For compliance, highly-specific, or cost-constrained offensive security testing:**
  - Penetration testing. Offering methodology driven testing, objective / outcome based testing, or high-level assessments.
- **For best-of-both-worlds:**
  - Bug bounty + penetration testing. Bounty for maximal vuln identification, and pentesting for compliance / coverage.
- **For fully customizable access to cybersecurity talent:**
  - Fractional Pentesting - pentesting talent how and when and where you need it. Pentesting on your terms.

OPTIONS, OPTIONS, OPTIONS ⌄

Congratulations! You've decided it's time to level up your security program in terms of identifying and managing security vulnerabilities, but how?

Here, we'll briefly outline the options that DarkHorse has to offer, and make some high level recommendations around what we think is the best fit, based on varying use cases.

THE OPTIONS, AT A GLANCE ⌄

1

Vulnerability Disclosure Program (VDP)

- **Is** a *passive* mechanism for independent third parties to be able to responsibly disclose vulnerabilities to your organization, across all assets.
- **Good for:** everyone. As a NIST & ISO standard, we believe that every org should have a VDP, and we back that belief up by offering VDPs for free.

2

Bug Bounty Program

- **Is** an *active* mechanism for independent third parties to report vulnerabilities and receive some form of compensation (monetary, swag, etc) for their work. Done right, bounties are the most effective means of identifying security vulnerabilities at scale.
- **Good for:** organizations that want to know about as many vulnerabilities in their attack surface as possible.

3

Penetration Testing

- **Is** the industry standard in offensive security. Can take on a wide variety of forms, including being objective-based, methodology driven, deep dives, or even higher-level assessments.
- **Good for:** meeting internal or external compliance requirements, ensuring coverage across a scope, testing highly specific scenarios, or cost-constrained, human-driven security testing.

4

Fractional Pentesting

- **Provides** on-demand access to pentesting talent, without having to purchase a full pentest. You specify how much time / effort you want invested, the methodology, skillsets, and artifact. We handle the rest.
- **Good for:** quick, ad-hoc security testing against any target.

Ready to get started? Get started in minutes at <u>darkhorse.sh</u>, or book a meeting at <u>darkhorse.sh/meeting</u>