Bug Bounty Programs
AT A GLANCE

1

How it works

The company defines which systems are in-scope and sets rules of engagement. Often organized through companies like HackerOne. Independent security researchers test the system.

2

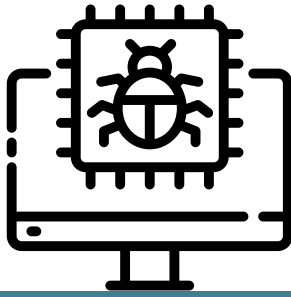
How it works cont.

Valid bugs are reported and fixed by the organization. For valid bugs, rewards are given based on severity and impact.

3

Advantages

Incentive alignment and cost-effective. Pay only for results. Diverse Expertise. Improved reputation, demonstrates proactive security culture building trust with users.



4

Disadvantages

Requires dedicated resources to triage and fix reported bugs. Quality of reports can vary. Cost uncertainty.

5

Who's doing it

Many companies, especially large companies have bug bounty programs like Google, Microsoft, Apple, Meta, and Tesla.

Sources

https://en.wikipedia.org/wiki/Bug_bounty_program

https://www.microsoft.com/en-us/msrc/bounty

https://hackerone.com/bug-bounty-programs