BASIC OF BUG BOUNTY

What Is a Bug Bounty?

Previously, the term “bug bounty” was used synonymously with the term “crowdsourced security.” With the arrival of additional ways to engage with a crowd, like penetration testing as a service (PTaaS) and attack surface management, the two terms have now been decoupled. Crowdsourced security is a resourcing model, while bug bounties involve an incentive (“pay for results”) model that encourages the discovery of severe flaws based on the potential for monetary rewards. For example, if a hacker involved in a bug bounty reports a cross-site scripting vulnerability but the same vulnerability was already noted by the customer’s internal security team or if it was uncovered by another hacker first, the individual is not paid for that submission. In another example, two hackers may uncover different types of server security misconfigurations. If one is email spoofing and the other is using default credentials, both hackers would be paid, but the latter would command a higher rate due to greater potential business impact. This model greatly reduces the average cost per vulnerability and ensures that customers are only paying for value received—which makes security return on investment (ROI) much easier to calculate.

History of bug bounty:

In 1851, Charles Alfred Hobbs was paid 200 gold guineas by a lock manufacturer for rising to the challenge of picking one of its strongest locks. Flashing forward to the mid-90s and early 2000s, Netscape, IDefense, Mozilla, Google, and Facebook all had their own self-managed bug bounty programs, offering severity-based rewards to anyone who could identify vulnerabilities in their web applications. Some organizations with large security teams and at an advanced stage of security maturity may still run their own bug bounty programs, but most that start in self-managed mode eventually migrate to “bug bounty as a service” solutions when they reach a certain scale. Generally, running bug bounty programs is outside the core competencies of most teams.

BASIC OF BUG BOUNTY

Who Participates in a Bug Bounty Program?

In crowdsourced security, “the Crowd” is the term used to refer to the massive, global community of hackers (also referred to as security researchers, ethical hackers, or white hats) who participate in bug bounty programs. These individuals are independent actors who work on crowdsourced security programs that they find to be fulfilling, lucrative, or both, either as their sole occupation or as a side hustle. The Crowd is the lifeblood of any crowdsourced security or bug bounty program and the main reason why the approach is so effective. Hackers can and do hunt bugs on multiple platforms—no provider has an exclusive monopoly on them—so it’s important for a platform to match the right crowd to the end user’s needs at the right time. Some crowdsourced security vendors boast a high number of hackers working on customers’ programs, but quality is a more important metric to focus on when working with the Crowd. Organizations want to be sure they’re working with a vendor that uses data to source and activate hackers with precisely the right skill sets and experience for their programs to boost engagement and critical findings—not just “throw bodies” at a problem.

What Motivates Hackers?

Per Bugcrowd's Inside The Mind of a Hacker report, 75% of hackers identify non-financial factors, such as personal development, the greater good, and enjoying a challenge, as their main motivators to hack. Only 29% of elite hackers hack full time, while the majority split hours between part-time hacking and full-time employment as analysts, engineers, and even CISOs. Furthermore, 77% of hackers work in IT or cybersecurity. The bug bounty community is a global group of wellintentioned individuals from all walks of life, with diverse backgrounds, technical skills, and expertise. The bug bounty community is a global group of well-intentioned individuals from all walks of life, with diverse backgrounds, technical skills, and expertise. Hackers go by a variety of names, but all share one critical trait—a desire to not only improve their families’ and their own lives but also to improve customers’ lives. This diversity is what makes bug bounties so impactful—the crowd offers the opportunity to connect uniquely skilled individuals with organizations that need fresh perspectives.

BASIC OF BUG BOUNTY