hackerone

Case Study

YAHOO!

Yahoo's Cutting Edge Approach for Protecting User Data

The Challenge

When you operate a platform that serves more than one billion users globally, even the smallest security issue can have a significant impact. Millions of Yahoo users could be affected by a vulnerability lasting minutes. Yahoo's security team - "The Paranoids" - protects Yahoo's users, as well as Yahoo's network and application space. Simply playing defense isn't enough in today's security landscape. To address this, Yahoo runs a bug bounty program, using reports from hackers to make tomorrow's code even safer.

Yahoo's security team innovates continuously so that Yahoo's software development process is leveraging secure code from the outset. For example, Yahoo uses proprietary code inspection tools to add an extra security layer to their DevOps. Yahoo partnered with HackerOne in 2013 to help scale their bug bounty program, and the company rewards security researchers for submitting vulnerability reports to the company.

"Security is an investment, and Yahoo has invested in some of the best pen testers in the business. But like any investment portfolio, it's smart to diversify. Today, one of the best investments a company can make is to crowd-source the best and brightest in the pen test community to find security issues before criminals do."

- Bob Lord, Yahoo CISO

The Solution

By relaunching their bug bounty program with HackerOne, Yahoo was able to obtain more actionable vulnerability information to feed back into their secure software development process. They have further improved user security and now have a more streamlined process for managing payments to security reporters.

Yahoo on HackerOne Quick Facts

- $1.6M+ paid to security vulnerability reporters.
- 12,000+ reports received
- 2,200+ reports have earned a payment
- 19% of reports receive payments - one of the highest among HackerOne programs.
- 2,200+ unique reporters
- 600+ reporters have found verified bugs

(Source: Yahoo, May 2016)

Reports came in immediately - over 15 per day - all tagged with hacker history and metadata and easily searchable through HackerOne. Individual bugs became case studies for teaching developers about better security coding. HackerOne aggregate data helped guide new practices and tool improvements. HackerOne's community of thousands of active hackers plugged into Yahoo's revamped bug bounty program, and now contribute to a vibrant and growing community of security reporters who search for high-quality vulnerabilities.

YAHOO!

The Results

To date, Yahoo has received over 12,000 reports and paid out over $1.6M for valid reports. Approximately 19 percent of these reports resulted in a payment to a hacker, with the remainder of reporters receiving direct communication and follow up after submitting their report. Over 2,200 hackers have participated to date, adding their experience and skills to aid Yahoo's Paranoids.

In addition to using HackerOne data to track the effectiveness of the bug bounty program, Yahoo also uses this data to provide insight into their software development lifecycle. By analyzing valid researcher reports and discovering vulnerability trends, Yahoo is able to perform root cause analysis to improve the security of their products and even mitigate entire classes of bugs. The feedback loop created with the HackerOne data helps Yahoo create and maintain more secure products for their users.

Yahoo's HackerOne program has been one of the most successful on HackerOne since its launch and regularly ranks in the Top 10 of all HackerOne customer programs. Yahoo was able to engage more hackers to lend their skills to The Paranoids, resulting in thousands of closed vulnerabilities.

