hackerone

Turning Security Inside Out

THE ZENEFITS BUG BOUNTY STORY

Tips for a successful private bounty program from one of the fastest growing companies in Silicon Valley.

CUSTOMER STORY

ZENEFITS

Customer Data

STATUS

Private

NO. REPORTS SUBMITTED

590+

HACKERS THANKED

40+

COMPANY SIZE

500 - 1,000 Employees

INDUSTRY

Healthcare / Software

There's nothing more important than protecting the lifeblood of your business: customer data

Zenefits, the All-in-One HR Platform, holds sensitive financial data for over 10,000 small and medium businesses.

That's a lot of high risk data, Personally Identifiable Information (PII), and Protected Health Information (PHI) for its customers. Thankfully, Zenefits has a world-class security program and team, and they know they must be on their game 24/7, much like many other companies with similarly sensitive data and brand reputation to uphold.

So what to do? Here are some tips from the Zenefits security team.

TIP #1

Plan for the best, expect the worst

What does it mean to be on your game 24/7? For the Zenefits security team, it's a culture of readiness and awareness. They know criminals are vigilant in looking for that loophole, that forgotten flash file, that open endpoint.

This knowledge drives their approach. "We had a good security track record", said former CIO Justin Calmus. "And that worried me." He continued, "Criminals love a false sense of security, so prepping for the next attack means looking like a prepper today."

To address the "ever-ready" demand of security, Zenefits embraces the belief that hacking is inevitable.

> I tell new developers that their code will be hacked. Tomorrow, maybe even later today.
>
> **- MACK STAPLES, SR MANAGER OF ZENEFITS RED TEAM**

"We're not just holding financial data; we're holding data on families and dependents. I protect that as if my own family's information were at risk," Mack continued.

This reflects a proactive stance of their security planning, treating every valid report like "this is how the attackers are thinking" and plan fixes in advance, rather than retroactively patch. Easier said than done, but an important mental approach to emulate.

TIP #2

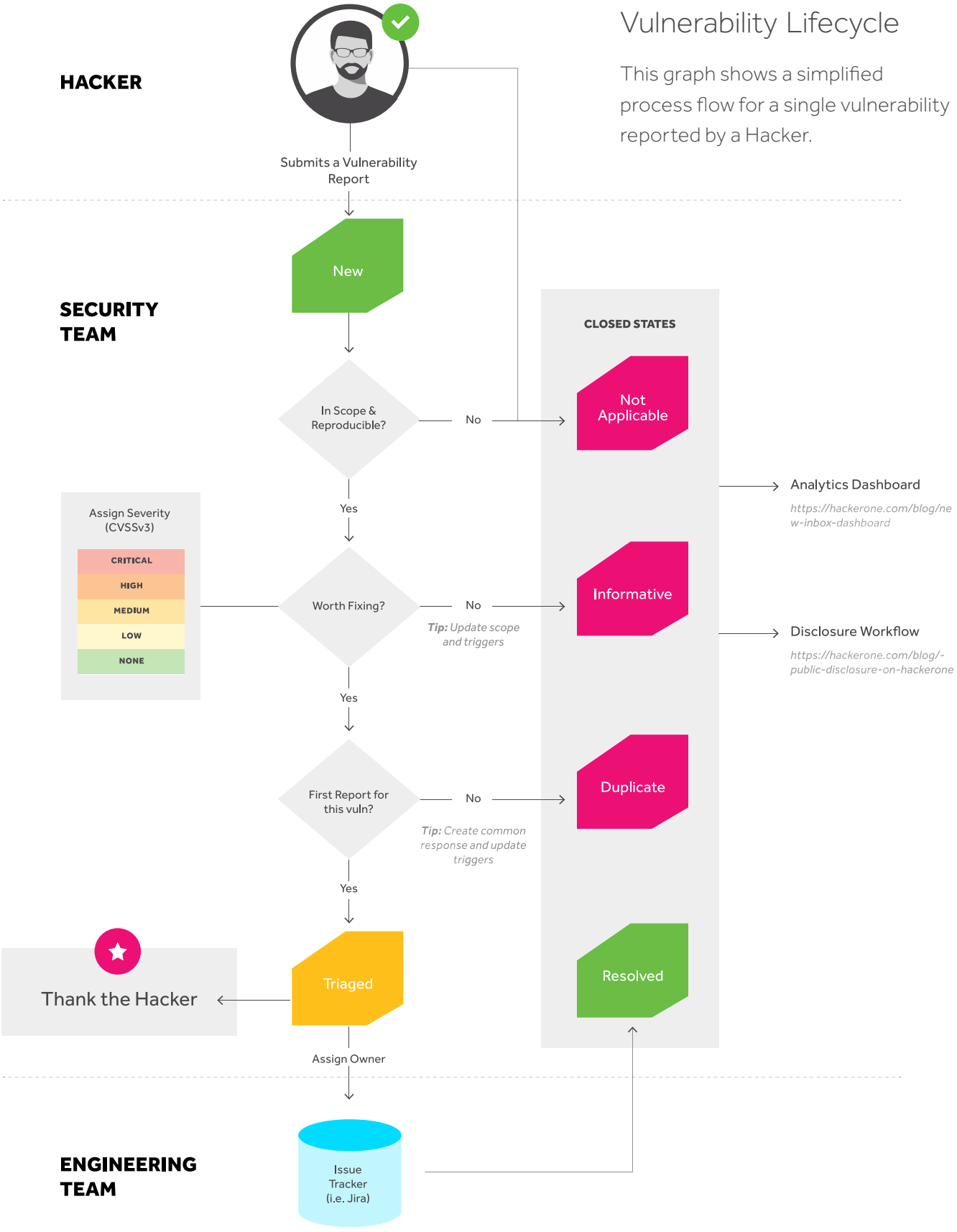
Partner closely with engineering and development teams

Security must always be "on", to respond to the dynamic environment all companies are facing today. That's why Zenefits loops their developers into the security process. Zenefits routes found vulnerabilities back to the initial development team to streamline code fixes. One way engineering can be fully integrated into your bug bounty process and triage flow is with the HackerOne API. With over a dozen teed up integrations, including ticket tracking systems like JIRA, following a bug report through to resolution is simple and aligned with your existing processes.

The goal is to get from valid report, through successful triage, and deploy a fix as fast as possible. Not trivial, but to visually see the process, we've mapped out those steps in the Vulnerability Lifecycle graphic.

Vulnerability Lifecycle

This graph shows a simplified process flow for a single vulnerability reported by a Hacker.



CALL IN THE EXPERTS FOR TRIAGE SUPPORT

Triage is one of the most important components of any bug bounty program. HackerOne's platform has the highest signal-to-noise ratio in the industry so you start from a higher reporting quality, but Zenefits found themselves in a position familiar to many companies: receiving lots of good reports, but falling behind in Triage. The solution? Zenefits was able to leverage HackerOne's team of research and triage experts to bring their queue current. 'It was an excellent service,' Mack Staples commented, 'and it helped us catch up. **We were the victim of our own success and had so many great reports that we needed a bit of a boost. HackerOne put some of their best on the task and they knocked it out of the park.** The team not only brought us current but was able to give feedback on the common issues they'd seen." See if triage assistance is right for your program by contacting sales@hackerone.com.

GET THE SCOOP ON TRIAGE →

TIP #3

Recruit and retain hackers that understand your business and tech and are willing to invest the time to test your logic

Vigilance against malicious attacks requires you to think like a criminal. For Calmus, an occasional hackathon organizer, the answer to tap into that thinking was clear: hackers. Not just any skilled hackers - they needed skilled Zenefits hackers.

To find those, they needed training and experience - all of which required a commitment to hack Zenefits instead of the other lucrative opportunities out there. They needed hackers who would hack and hack again, knowing that the most severe - and therefore valuable - vulnerabilities come from repeat and ongoing hacking.

So the question then is, "how do you recruit top hackers to focus on your company?" One simple way to focus your initial efforts is inviting hackers based upon reputation and validated skillset, a feature which is available in the **HackerOne Professional** tier. The longer answer to this question leads us to tip #4.

TIP #4

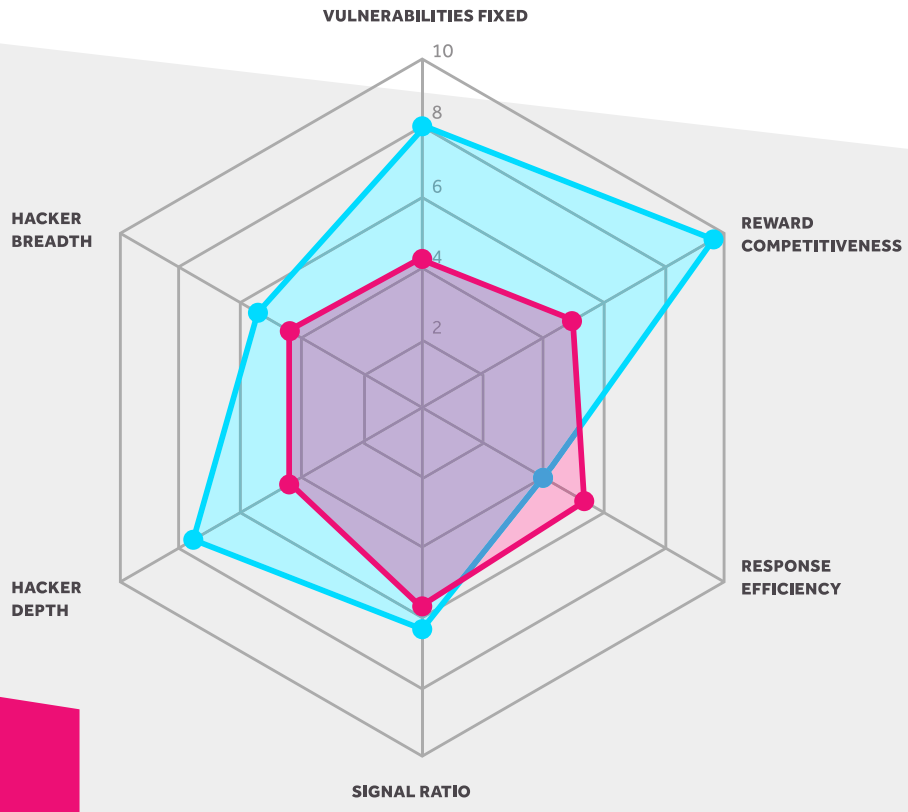
Maintain a competitive and generous bounty program

To attract the best hackers, Zenefits set out to create one of the most attractive bug bounty programs in the world.

With multiple $30,000 awards, they are the highest awarder on the HackerOne platform. Zenefits' average hacker (defined as submitting at least one bug) has earned over $8,000.

How Zenefits' bounties compares to avg Enterprise.

- Zenefits
- Avg. Enterprise



ARE YOU READY FOR A BUG BOUNTY PROGRAM?

Click here to get your org's maturity model score. →

As you can see, Zenefits reflects quite favorably in the key measurements we track for all programs. What do each of these mean? Let's dive into some definitions for further clarity:

VULNERABILITIES FIXED

number of vulnerability reports resolved, breadth of vulnerabilities resolved

REWARD COMPETITIVENESS

average bounty, number of bounties, bounty award structure, maximum bounty

RESPONSE EFFICIENCY

report close time, first response time, bounty time, triage time.

SIGNAL RATIO

percent clear signal, percent nominal signal

HACKER DEPTH

sum of contributor reputation, number of repeat contributors

HACKER BREADTH

number of new and existing contributors, public program

**For more on the HackerOne Success Index, see our blog:*
Measuring Success in Vulnerability Disclosure

Other techniques and strategies Zenefits employed included loyalty, creativity, and responsiveness. All part of the best practices playbook for running a successful bug bounty program.

Be loyal

By keeping their program private and slowly adding hackers, there's enough opportunities for all their hackers to find significant vulnerabilities year after year. Using HackerOne reputation scores, they were able to target only the best hackers. Repeat hackers produce better results; they know the software better. "My number one piece of advice for someone starting a bug bounty program is: Be Fair. That means ignoring your scope sometimes and rewarding a great hack," offered Staples.

Celebrate the creative hack

When one hacker, who had built an endpoint scanner, noted a new node on Zenefits attack surface, the security team was surprised. Sure enough, a developer put out a public, unpublicized endpoint. Zenefits was amazed and happy to have a teaching moment for their developer.

PRO TIP:

It's easy to pay hackers from anywhere in the world through the HackerOne platform. And you can even setup incentive-based bonuses to encourage hackers to really "wow" you.

Remember the ABCs

"Always be closing"... bug reports that is. A great response time shows hackers you mean business and are diligent in reviewing reports in a timely fashion. The HackerOne platform statistics provides valuable insights to Zenefits, giving them the data they need to gauge responsiveness.

And a great turnaround time further improves your odds of getting the best hackers to look into your business.

Get Started With Your Bug Bounty Program Today

hackerone

Making the Internet Safer Together

SOME OF OUR CUSTOMERS

slack UBER Square New Relic. GM Dropbox HACK THE ARMY

WWW.HACKERONE.COM / SALES@HACKERONE.COM / +1 (415) 891-0777