

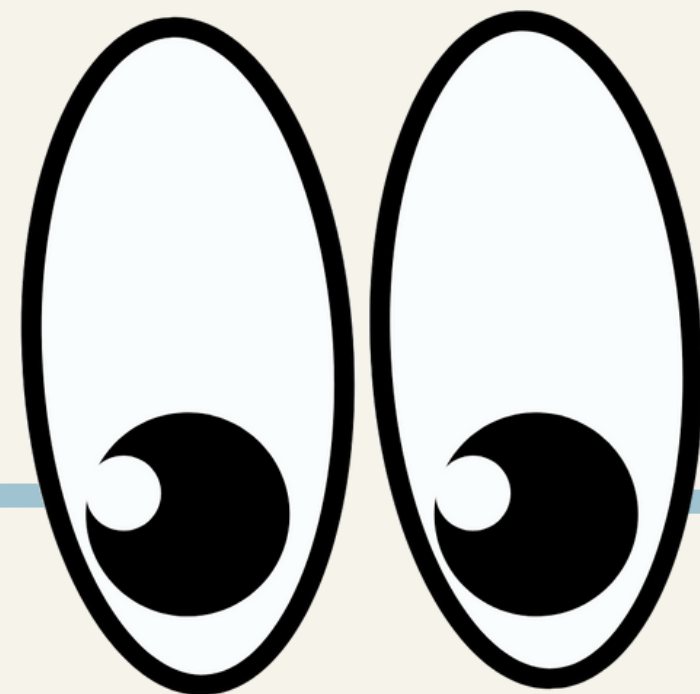
BREAKING BUILDS

Without breaking hearts

Tara Whitehead |  /tara-whitehead/



NO PEEKING!

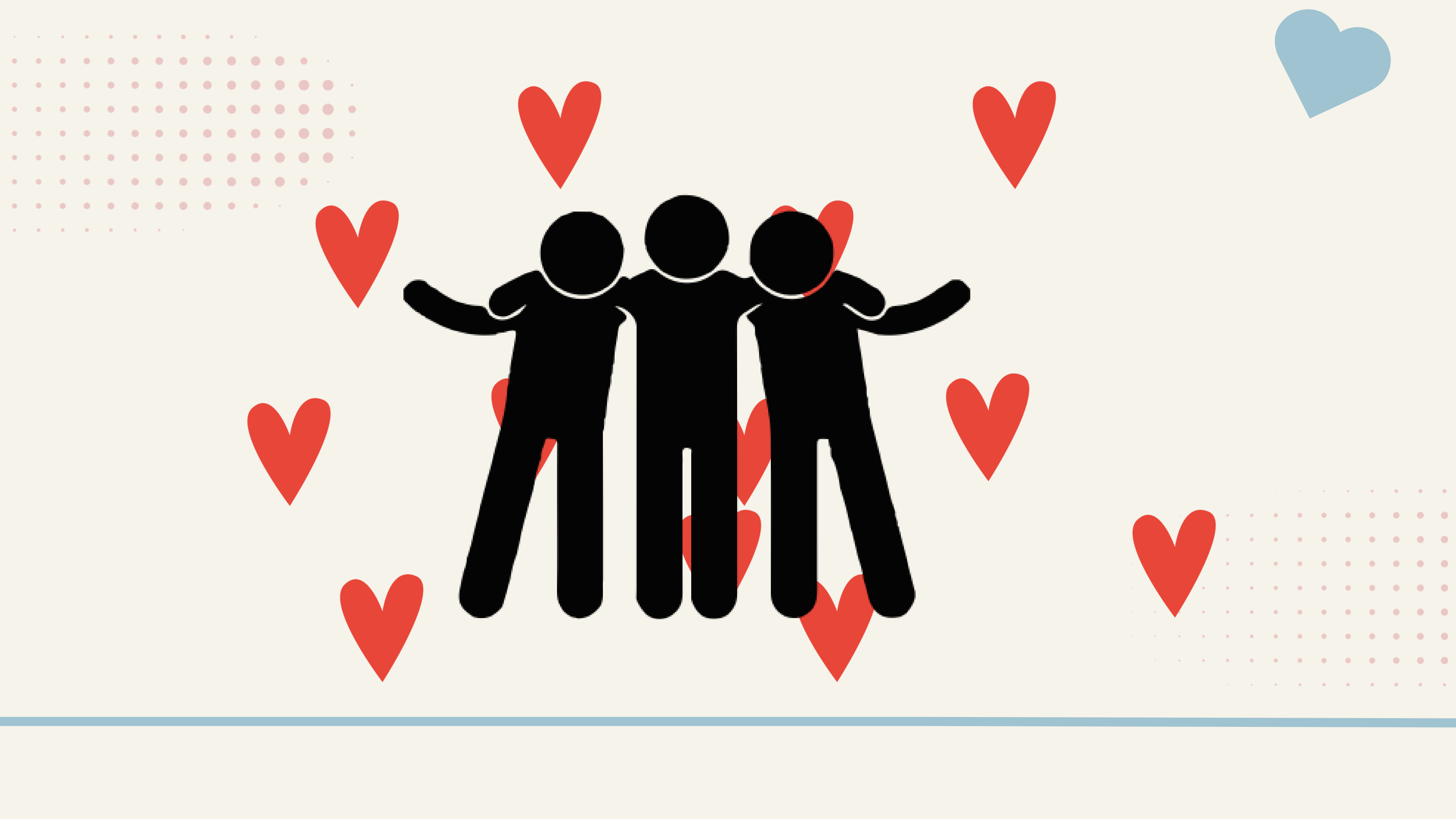




EMBRACE THE BURN









**Once upon a time in a
galaxy far, far away...**



PROS

- Powerful
- Significant coverage of Vulns
- Industry fan fave

CONS

- Horrible UX
- \$\$\$\$\$\$\$\$\$\$.....\$\$\$\$\$
\$\$.....\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
\$\$\$\$\$\$\$\$\$\$\$\$\$...\$\$\$\$\$



CONS

- **Not as Powerful**
- **Less Vuln Coverage**
- **Not even a SAST tool**

PROS

- **Free**
- **People actually used it**



**Change management begins
when you are looking at the
tool or service...**

**Not after you have already decided
the direction**



NEW BOSS,




NEW RULES

A large, stylized green leaf graphic with a textured, watercolor-like appearance, serving as a background for the text.

700 PEOPLE
60 DELIVERY TEAMS
4 BUSINESS UNITS

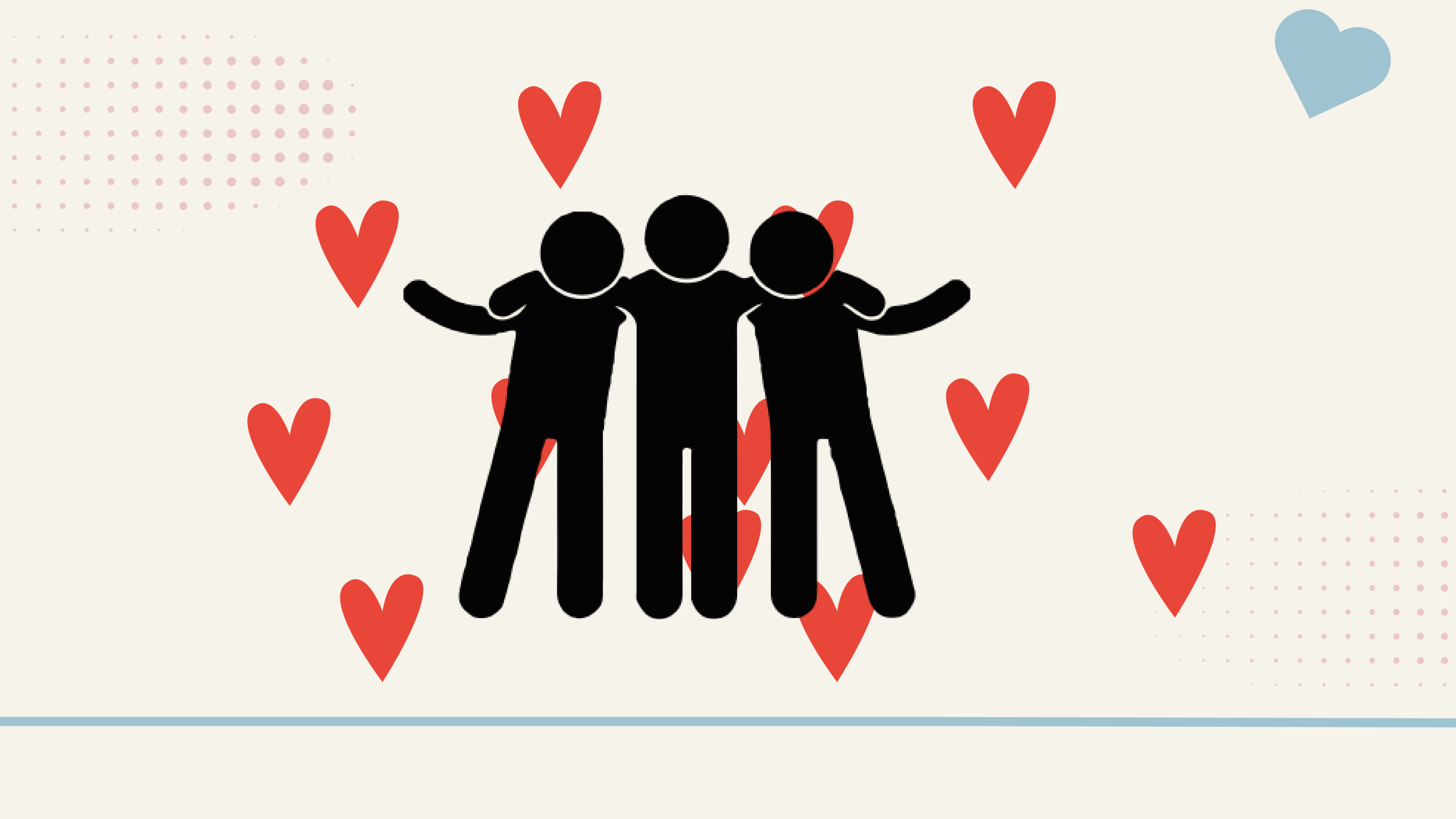


TEAMWORK!



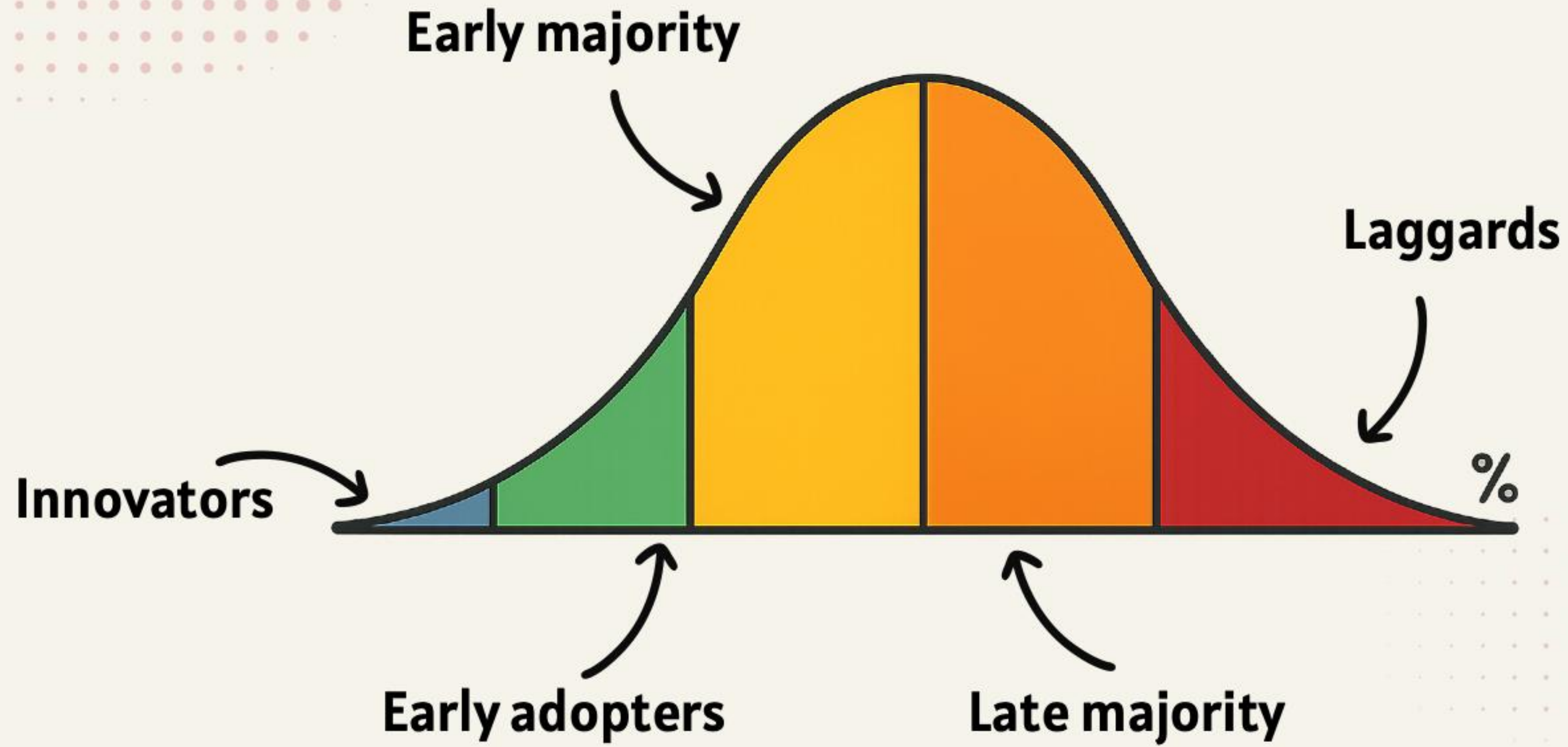
**Onboard everyone to
SonarQube...**

**And introduce a quality gate
into pipelines to ensure that
everyone would use it**





- 1** Legacy code not supported by SonarQube were pushed to a later version
- 2** Monstrously large codebases that took days to scan had a bespoke solution for a later version
- 3** We drew a line in the sand - only newly committed code from after the quality gate was installed would break build on failure to pass
- 4** We gave the people SonarLint





WIIFM?

♥ Hook 1

Shift left - spend less time fixing vulns in the long run

♥ Hook 3

Fix the vulns as you write the code, not when you can't quite remember how it works again?

♥ Hook 2


Why do you want to commit new Vulnerabilities to your code?

♥ Hook 4

Empowers devs to have better conversations when their work is ready



CHANGE MGMT STEPS

- 1** Have a great team that trusts and works with each other well
 - 2** Talk to your stakeholders - don't just assume!
 - 3** Find your change champions and leverage their enthusiasm
 - 4** Learn what works (and doesn't work) during the roll out and be agile
- 
-

The background features three vertical bars on the left: a wide pink bar, a medium blue bar, and a narrow beige bar. On the right side, there are two rectangular areas filled with a grid of small pink dots. The text "THANK YOU" is centered in a bold, black, sans-serif font. A light blue, cloud-like shape is positioned behind the letters "YOU".

THANK YOU