Maintaining a Security Champions Program
What is a security champions program?

A way to scale a security initiative by involving department members who don’t have formal cybersecurity experience.
Why is the program needed?

- Developers view security as a blocker
- Developers don’t understand AppSec
- AppSec doesn’t always know the application
- AppSec is generally outnumbered
The honeymoon phase

- Define the program
- Get management buy-in
- Identify & Onboard Champions
- Secure all the code
- Live a happy and rewarding life
Barriers

• Developers view security as a blocker!!!
• Developers don’t understand AppSec!!!
• AppSec doesn’t know the application!!!
• AppSec is generally outnumbered!!!
If it’s not working... Pivot!

- Survey champions
- Meet individually monthly
- Adopt hands on training
- Partner to set goals for each champion
- Make them feel like they are special
What didn’t work for us

- Volunteering developers to be a security champion
- Security training courses
- Setting expectations prior to starting the program
Set Maturity Goals

Where is our current maturity?
Where do we want to be?
How to we plan to get there?
Value your champions

• Involve them in POCs
• Get their feedback regularly
• Connect them with strategic teams
• Recognize their contributions
When it works, it works!

• Developers started reaching out to us with questions
• Developers started asking about the program
• Developers start talking about security amongst themselves
The social element

Be honest with your security champions

Don’t shame them when they are honest