Distributed Security Champions: working for developers

Presentation to Bristol (UK) Chapter
30th September 2025

OWASP®

OWASP FOUNDATION

Who am I?

- C/C++ developer for 25 years
- Security engineer for over 12 years

But more importantly:

- Leader & contributor to OWASP Threat Dragon project
- Co-leader & contributor on OWASP Developer Guide project
- Co-Leader of Bristol (UK) OWASP Chapter

Context:
Secure Development Lifecycle

- Security requirements
- Third party libraries / software composition analysis (SCA)
- Secure coding
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Application Security Verification
- Pentesting

so we get a security engineer to do all this, right?

Context:
the problem with Nutella

Generalising:

- Large companies may have security engineer ratio1:200
- Small and Medium can have less
- Security engineers are (still) hard to come by
- CVEs are increasing year on year

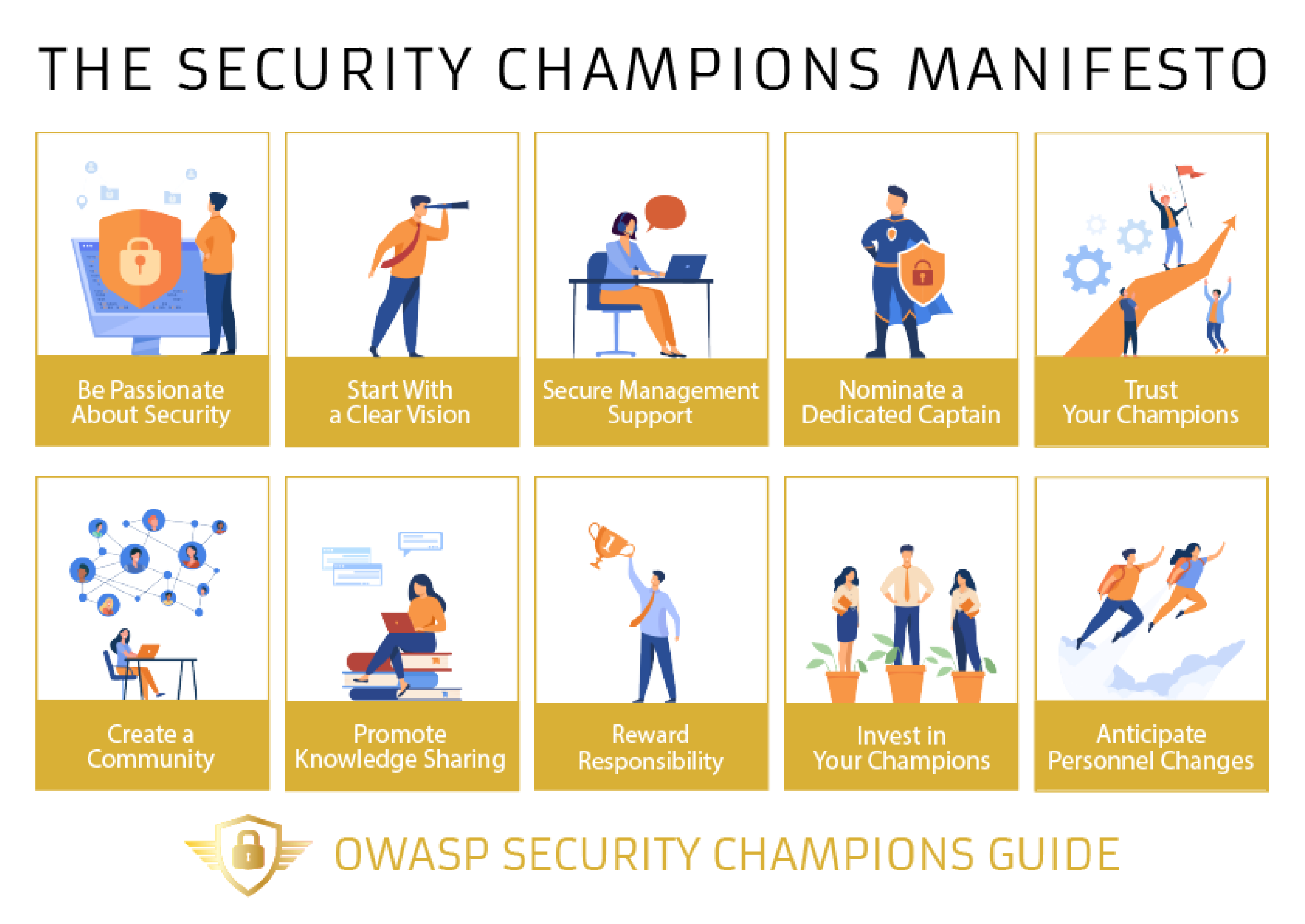
if this was a war, then we are not winning it

Security Champions to the rescue!

- Self selected by and from the development team itself
- Can be a developer - could also be QA, project manager, etc
- Bridge between Dev team and AppSec team
- Trained in security activities
- Knowledgable evangelist

OWASP
SECURITY CHAMPIONS
GUIDE

OWASP Security Champions Guide



THE SECURITY CHAMPIONS MANIFESTO

- Be Passionate About Security
- Start With a Clear Vision
- Secure Management Support
- Nominate a Dedicated Captain
- Trust Your Champions
- Create a Community
- Promote Knowledge Sharing
- Reward Responsibility
- Invest in Your Champions
- Anticipate Personnel Changes

OWASP SECURITY CHAMPIONS GUIDE

What is a Security Champion?

- Receives training and conference places
- Ensure the security activities are correctly applied:
  - Security requirements
  - Third party libraries / software composition analysis (SCA)
  - Secure coding
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
  - Application Security Verification
  - Pentesting
- Can it work? Well, you are looking at one :)

Can anything go wrong?

Can anything go wrong?

Yep, lots

Can anything go wrong?

- *Burn out* - in addition to their ‘day’ job
- *Leave* - highly trained → highly transferable
- *Self selecting* - not everybody is interested
- *Expensive* - training and conferences

Distributed Security Champions

Definition:

- A Security Champion ensures that security activities are correctly applied to the application or product. To do this they receive training and attend conferences with support from the company Security Champions Program
- A *Distributed* Security Champions Program is where these activities are shared out among the members of the development team. Training is given to the individual members according to what security activity they are responsible for

Distributed Security Champions

- Avoid burn out: security is now everybody’s responsibility
- Retain talent: share the training, share the satisfaction
- Equitable: do not rely on ‘security heroes’
- Affordable: more money for individual training

OWASP™