Contributing to OWASP projects

Presentation to Bristol (UK) Chapter

Who am I?

- C/C++ developer for 25 years
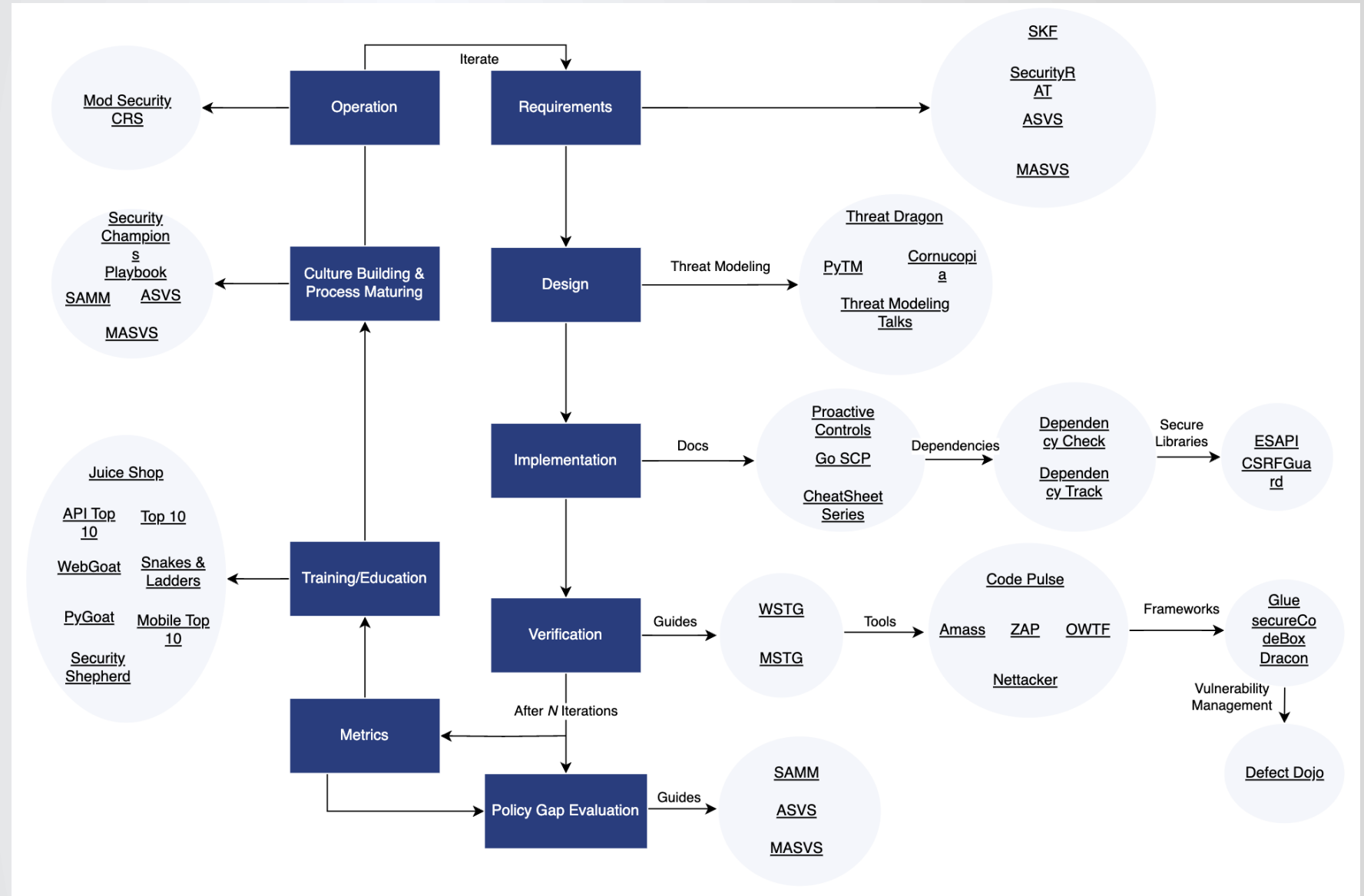- Security engineer for 11 years

But more importantly:

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

OWASP projects

- There are a lot of them ~302, classified as:

- 15 Flagship projects, eg WSTG

- 5 Production projects, eg CSRFGuard library

- Lab projects

  - 71 'Code' projects, eg Threat Dragon

  - 60 Documentation projects, eg OWASP Cheat Sheets
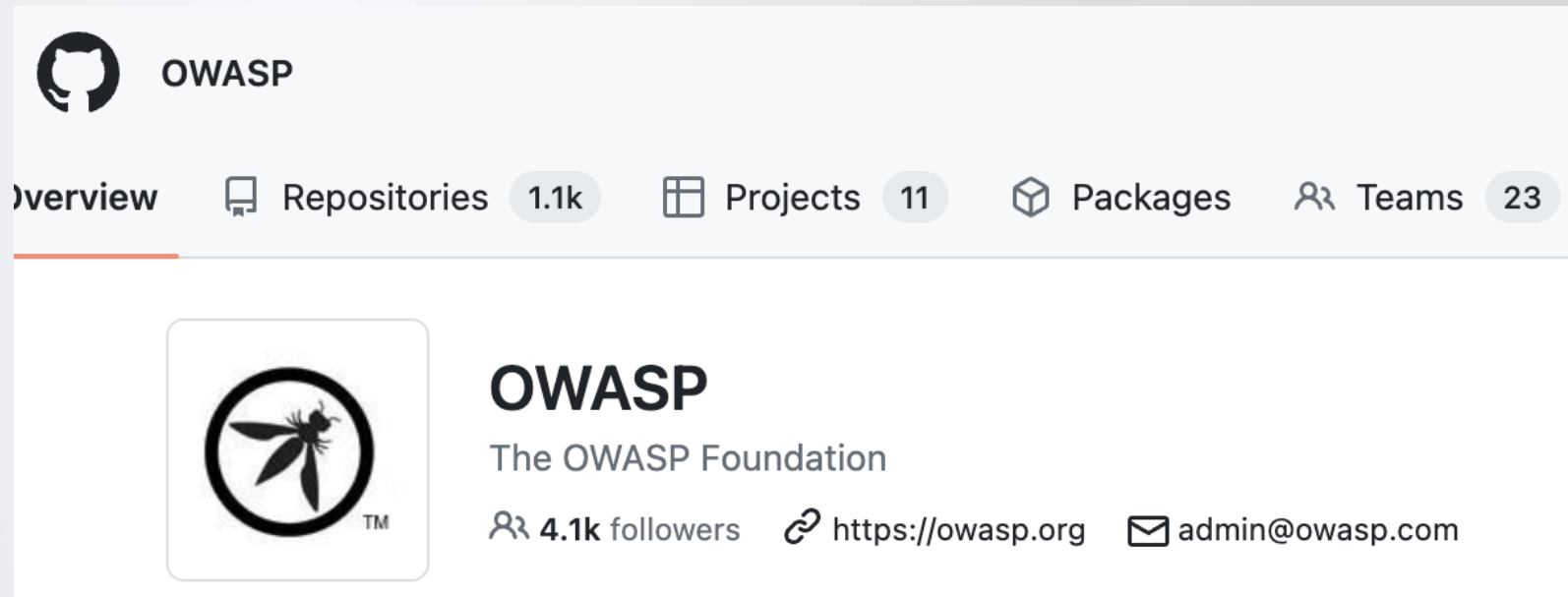
- Incubator projects

OWASP Project Wayfinder

owasp.org/projects/

Operation

Mod Security CRS

Requirements

Iterate

SKF

SecurityRAT

ASVS

MASVS

Culture Building & Process Maturing

Security Champions Playbook

SAMM   ASVS

MASVS

Design

Threat Modeling

Threat Dragon

PyTM   Cornucopia

Threat Modeling Talks

Implementation

Docs

Proactive Controls

Go SCP

CheatSheet Series

Dependencies

Dependency Check

Dependency Track

Secure Libraries

ESAPI

CSRFGuard

Training/Education

Juice Shop

API Top 10   Top 10

WebGoat   Snakes & Ladders

PyGoat   Mobile Top 10

Security Shepherd

Verification

Guides

WSTG

MSTG

Tools

Code Pulse

Amass   ZAP   OWTF

Nettacker

Frameworks

Glue secureCodeBox Dracon

Vulnerability Management

Defect Dojo

Metrics

After N Iterations

Policy Gap Evaluation

Guides

SAMM

ASVS

MASVS

OWASP repositories

- Mostly as code and documentation markup
- Github OWASP organization github.com/OWASP
- Over 1100 repos
- Submit by pull request
- Join the community!

Why do it?

- For the pleasure of contributing to the open source community?
- Opportunity to do that coding you always wanted to do?
- Your company really needs that tool?
- Respect from your peers?
- Looks good on your CV?
- Trust = credibility + reliability + intimacy + alignment

What is it like?

- But the world can see my code!

    - yes, but you are within a supportive community
- How do I know what to do?

    - every project has open issues with tags
- Where can I start?

    - the flagship projects are busy; try lab / incubator projects
- Will it take over my life?

    - maybe ;)

Case study: Developer Guide

Along with the OWASP Top Ten, the Developer Guide is one of the original resources published soon after OWASP was formed in 2001

Version 1.0 of the Developer Guide was released in 2002

Last version was 2.0 in 2005

Developer Guide: contribute

"I am a developer; I need a reference source to navigate the numerous OWASP projects, which also provides an introduction to the activities that I am supposed to be doing"

Contributions welcome