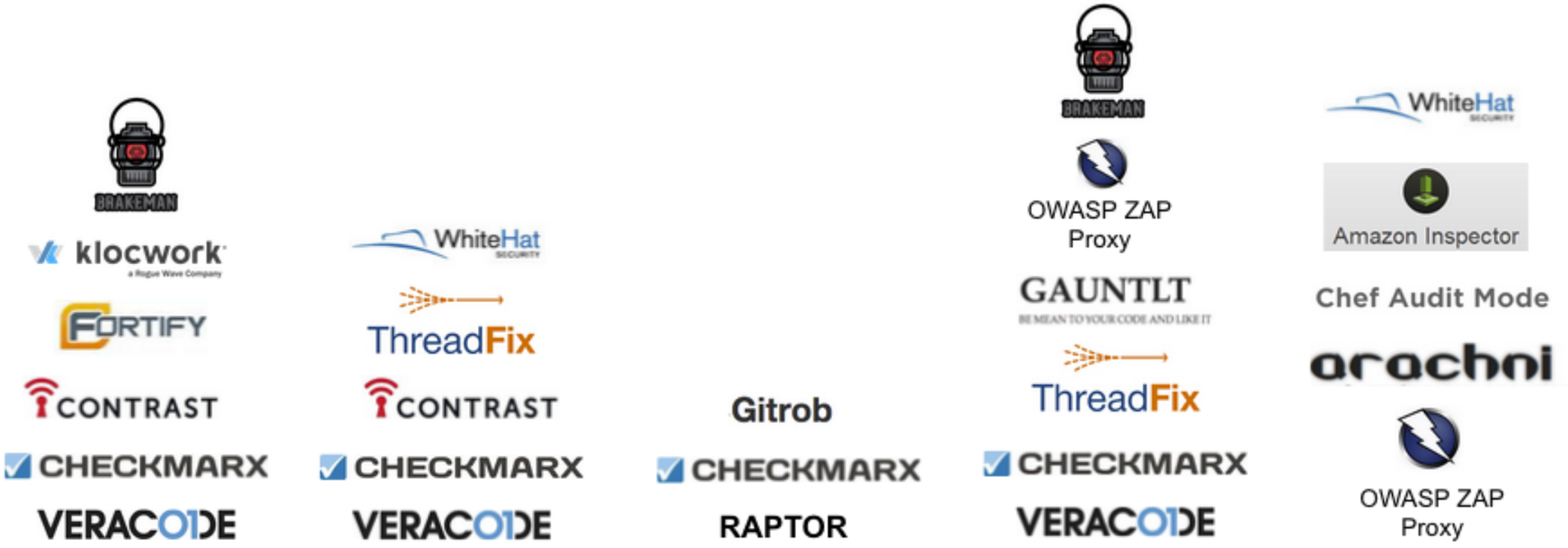
- OH MY - H@CK

# How to support developers in secure coding?

Adrian Sroka, Software Security Architect

# How we usually care about the security?





Code | Manage | Store | Build | Deploy

# Who can best take care of application security?

Developer

Why?

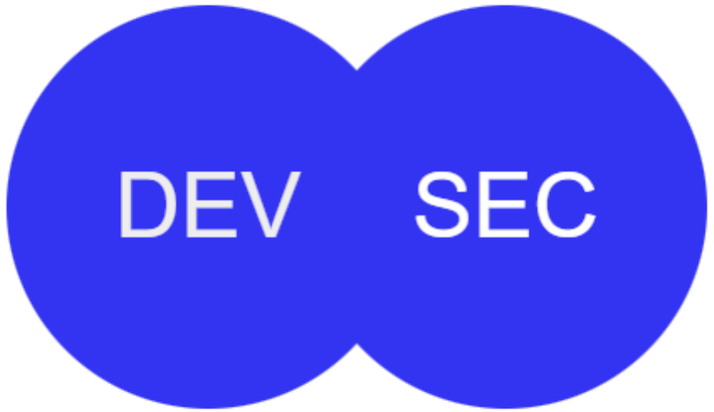
They have the best domain and technical knowledge

But...

They are not a security expert

# Dev + Sec – starting point


# Dev + Sec – target point



# How to implement security effectively?

1. People
2. Processes
3. Tools

In this particular order

# How we can help developers?

# Training

Popular scenario

1. Everyday regular work
2. Security training
3. Initial excitement and interest
4. After a few weeks, they don't remember much of it.

Not very effective

# Problems with automated checks

- DAST – small domain and technical knowledge
- SAST – narrow scope of analysis
- SCA – important, but it doesn’t look on code

# The biggest challenge in security for developers?

- They don’t feel comfortable in it
- Lack of time, to learn and experiment
- As a consequence – they don’t keep the rules

# How we can help them?

- Let’s make it natural for developers

But…

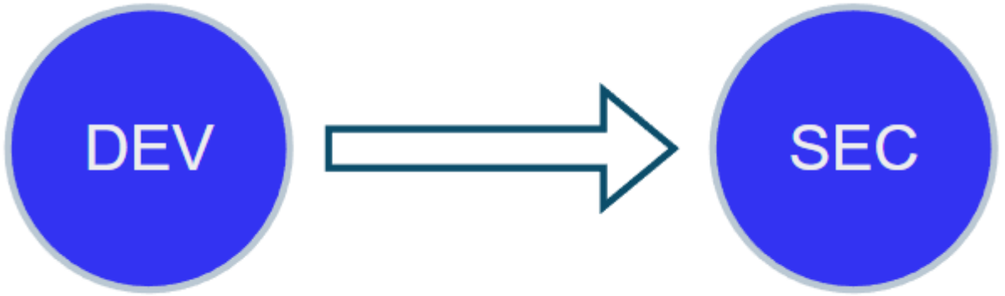
- Easy to tell, hard to achieve

# 5 steps to help developers be fluent in security

It could be easy

Disclaimer

- Based on experience and experiments
- Subjectively



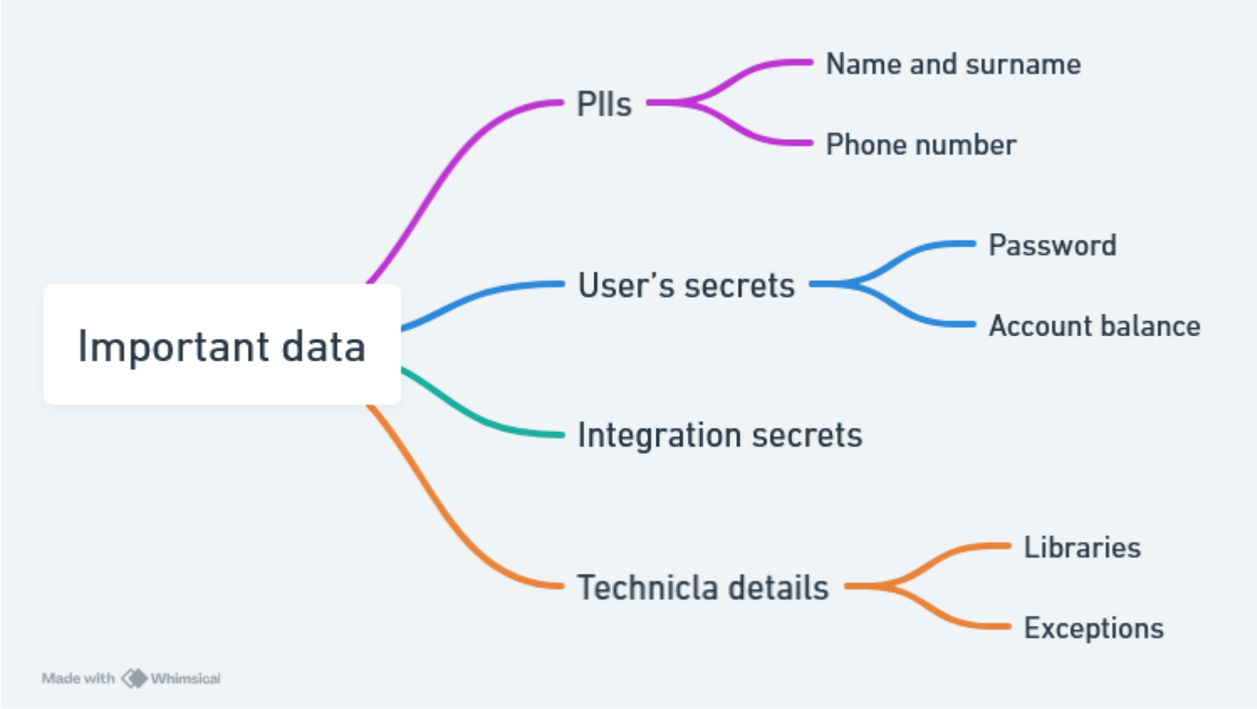

# 1. Build awareness of important security areas

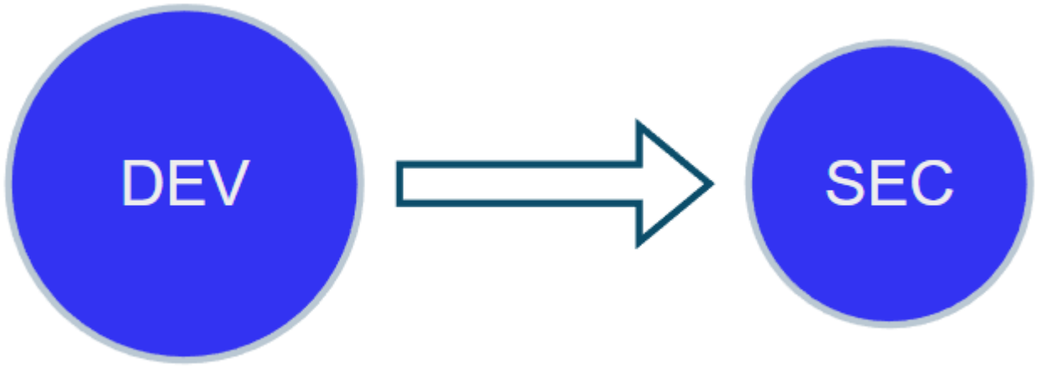
Developer: I don’t have to know how to fix the problem, it’s enough to know in which situation I should raise an alarm and ask

# Build awareness of important security areas

Building a security map:

- areas
- data
- functions






# 2. Facilitating decisions

Developer: Even if I don't know what will work best, I know where I can find help

# Facilitating decisions

Types of decisions

- choice of technology
- libraries
- algorithms
- good practices

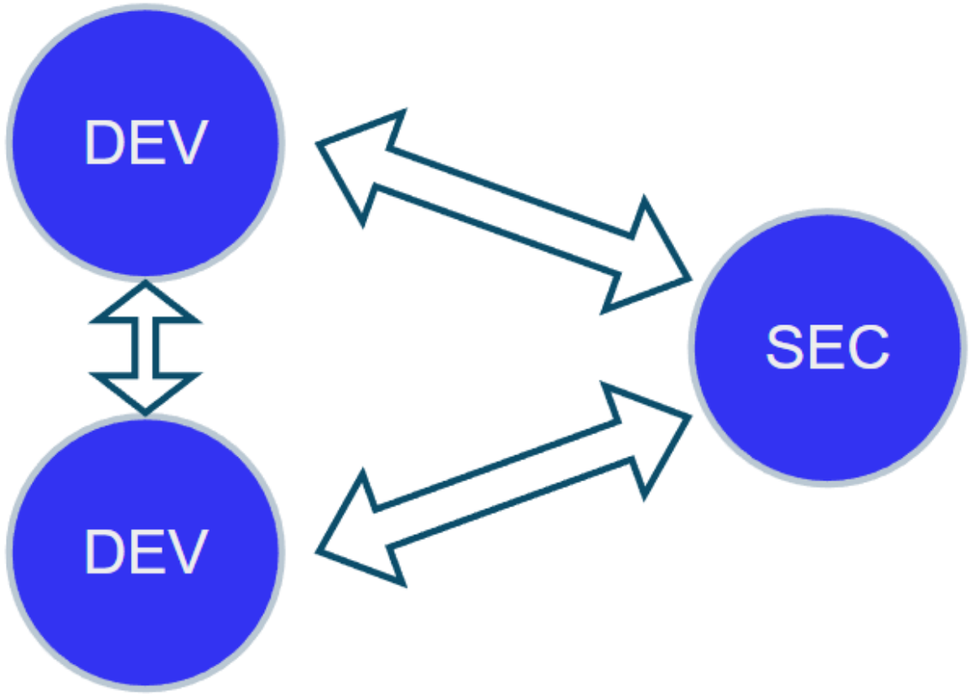
# Facilitating decisions

Automate decisions the same way you automate tests

Tools:

- checklists
- knowledge bases
- mental models
- policies

| If functionality is related with… | … and … | … ask following questions |
|---|---|---|
| Backend | Files | Do we validate files during upload?<br>Do we have an antivirus scan? |
| | Exceptions | Do we hide any technical details on errors? |



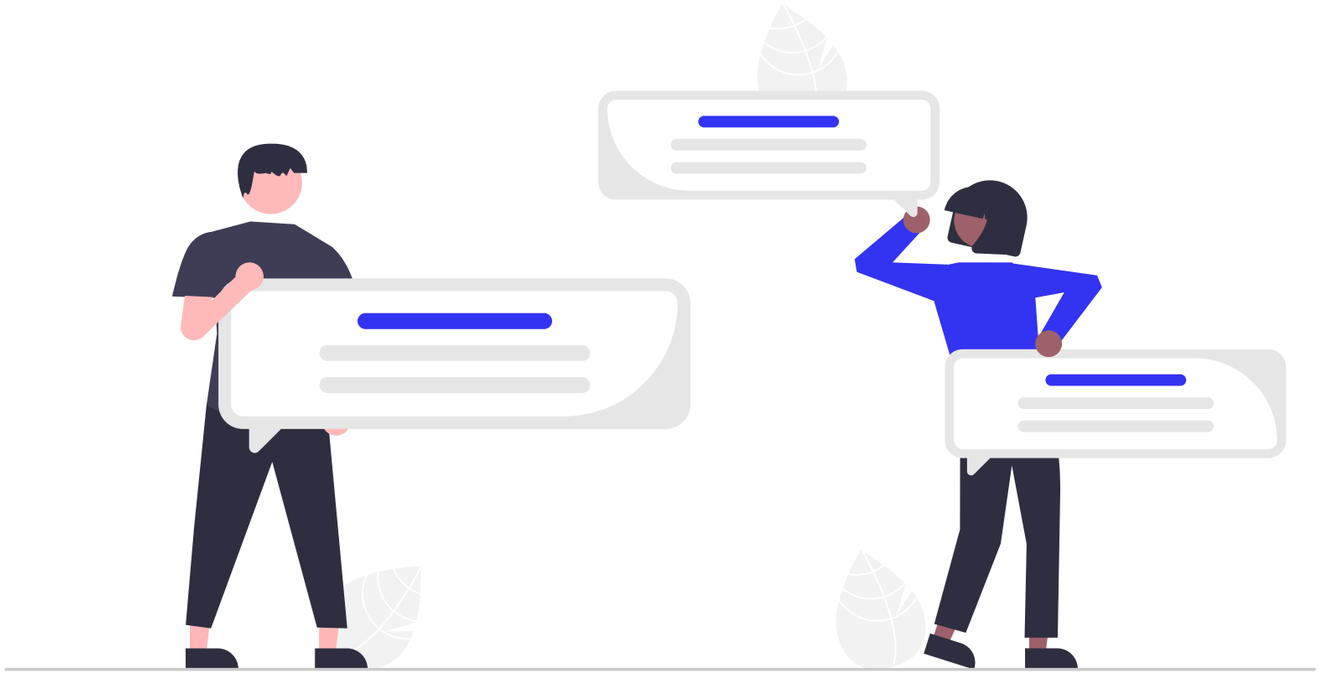

# 3. Discussion place

Developer: I always have someone to turn to with my problem

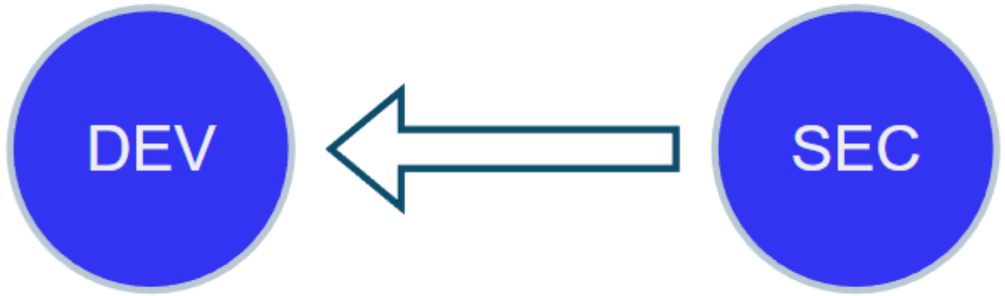
# Discussion place

Building a community

- within team
- within company



It is good that they identify problems and wants to talk about them




# 4. Regular exposure

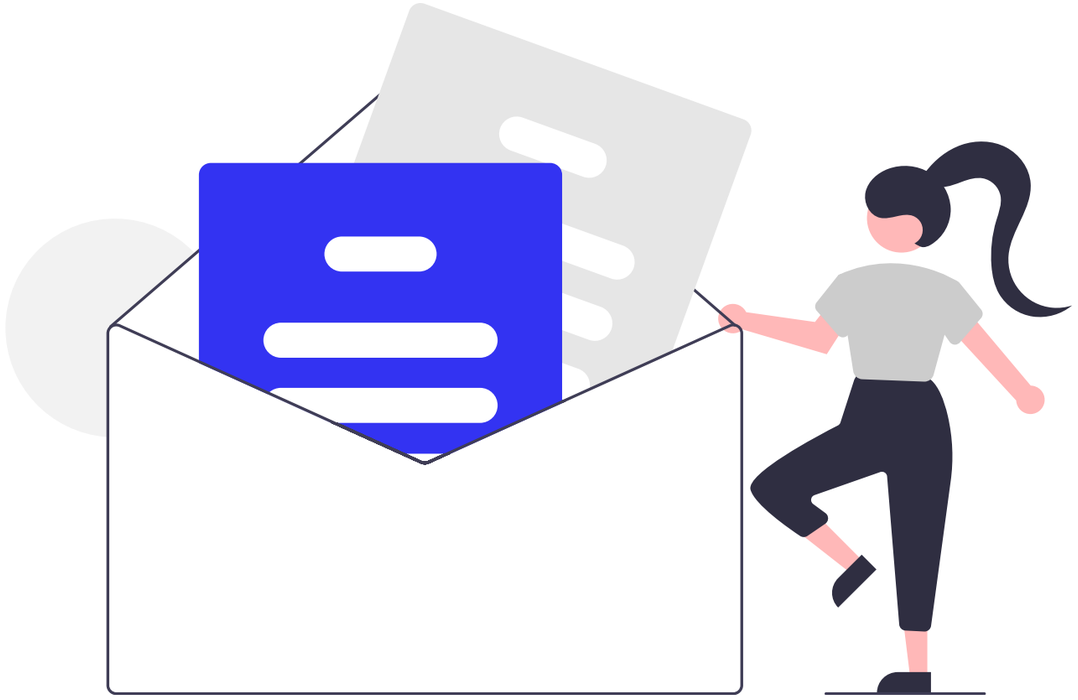
Developer: I systematically hear about security and what is happening in the company around this topic

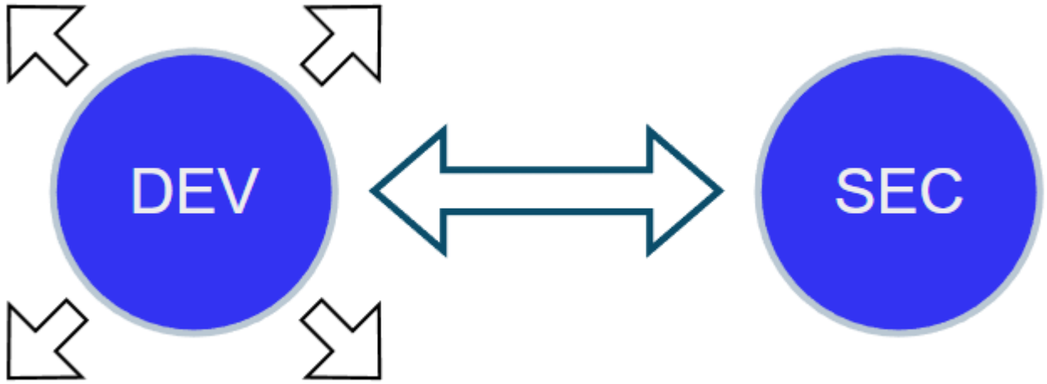
# Regular exposure

Reminders

Newsletters

Transparency of activities



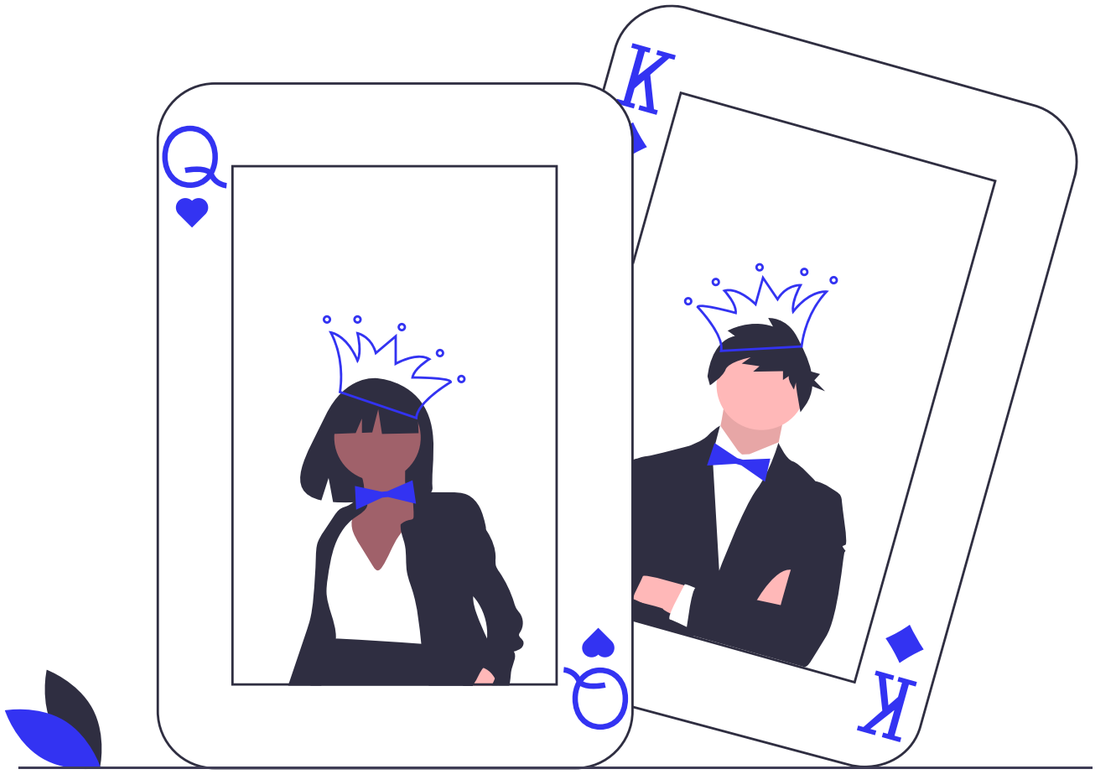



# 5. Engagement

Developer: I can regularly verify my knowledge and test new ideas

# Engagement

- Opportunities to prove yourself
- Shared challenges
- Hackathons
- Exercises
- Involvement in decisions
- Given responsibilities



# 5 key elements

1. Build awareness of important security areas
2. Facilitating decisions
3. Discussion place
4. Regular exposure
5. Engagement

# Recipe

It’s a recipe for Security Champions Program

# Security Champions

A community of people interested in security

What problems does it solve?

- Scaling - Security specialists cannot be in every team
- Eliminates distance - brings developers and security together

# Security Champions – how to establish it?

# Security Champions – how to do it right?

How do you keep the interest?

- They are up to date with what is happening in the company
- They know more than others
- They have more opportunities