Tanya Janca

SheHacksPurple

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

Security Champion *Worst* Practices

Tanya Janca (SheHacksPurple)

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

What are we going to talk about today?

Security Champion Programs

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

What are we going to talk about today?

What can go wrong

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

What are we going to talk about today?

How to do better

Spoiler:

Security champion programs are all the rage right now, but they aren't a magic bullet; they are a lot of work and more than half of them fail.

Thesis:

Most people start a program to reduce friction, scale their program, and improve culture and communications.

But teams rarely give clear and realistic direction to their champions and do not achieve their goals.

BARCELONA

Let’s go!

The mandatory ‘about’ me slide.

Tanya Janca

- Staff Developer Relations at Semgrep
- AKA @SheHacksPurple
- Secure Code Trainer
- Author: Alice and Bob Learn Secure Coding &

  Alice and Bob Learn Application Security
- 28+ years in tech, Sec + Dev
- Founder: We Hack Purple, OWASP DevSlop,

  #CyberMentoringMonday, WoSEC
- Advisor: Katilyst
- Faculty: IANs Research

How I did my research

Surveys
Social media
Working with ~~50~~ 54 clients
Building two programs personally
Interviews with experts


AI is reliably *wonky*
Spot the creepy

Agenda

1. Why Champions?
2. What goes wrong and how to do better
3. Conclusion

Why Champions?

Reduce Friction!

Why Champions?

1. Scaling the security program and internal expertise
2. Shifting left -> saving money
3. Security culture improvement
4. More proactive developers
5. Security incidents reported faster, or avoided
6. Increased Sec + Dev engagement
7. Hiring champions to the security team
8. Higher moral for champions and lower absenteeism

Scaling the security program and internal expertise

Shifting security left saves money

Anywhere from incremental improvement to a complete transformation in security culture and a more proactive mindset.


Increased proactivity from developer teams, leading to more bugs being fixed.

Faster, more reliable security incident reporting helps reduce cost, embarrassment, and overtime requirements.

Trust and friendly relationships built between sec and dev

Avoiding security incidents altogether! WIN!


Hiring for the security
team, from the champions

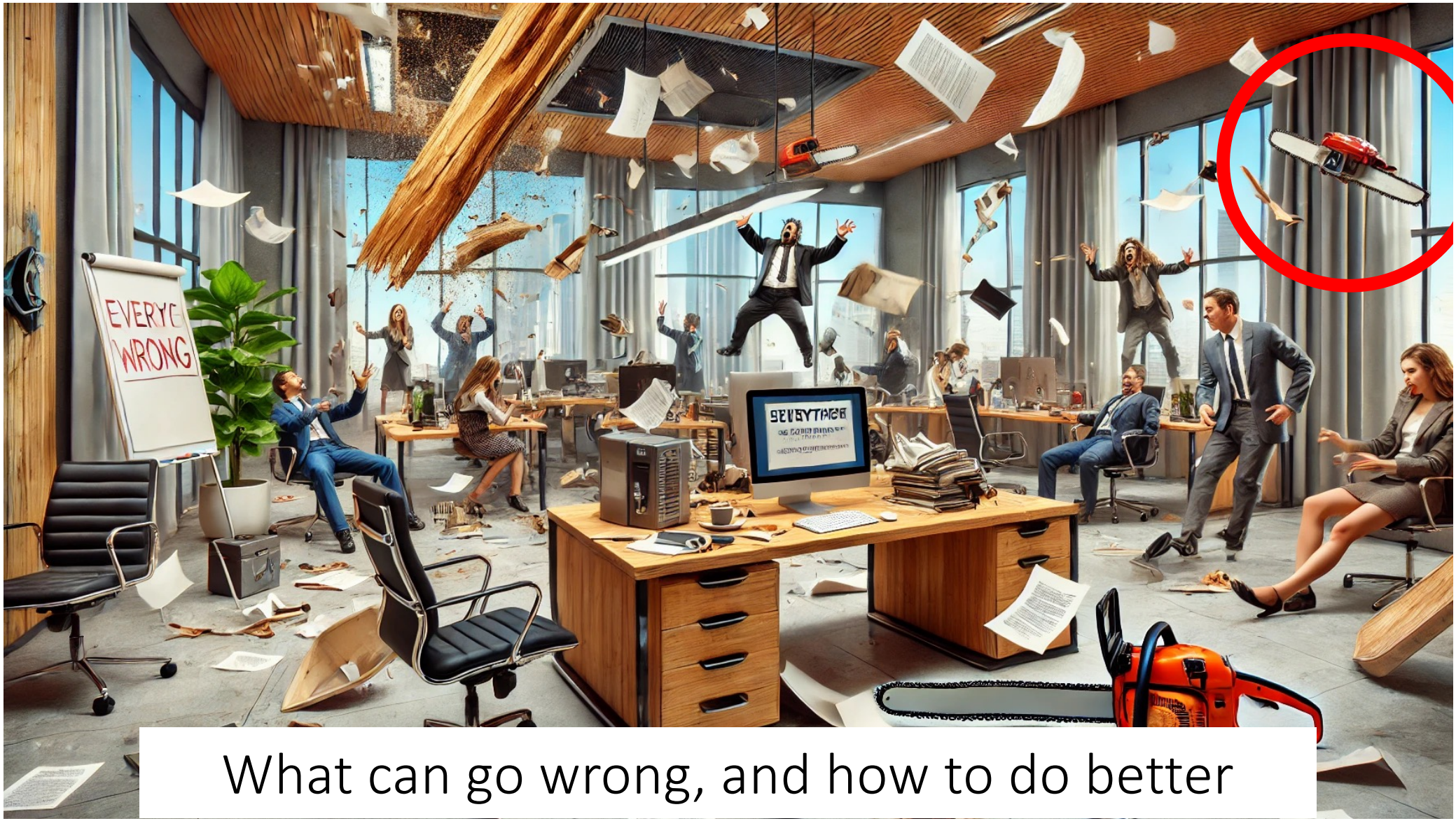

Influx of security related questions and concerns to the sec team, helping them reduce organizational risk and increase engagement.

rple


Champions have higher work satisfaction and lower absenteeism.

Agenda

1. ~~Why Champions?~~
2. What goes wrong and how to do better
3. Conclusion



What can go wrong, and how to do better

What can go wrong, and how to do better

1. Unmaintainable pace
2. Unclear responsibilities
3. Involuntary volunteers
4. Failures in recruitment
5. Unrealistic responsibilities
6. No top-down support
7. Lack of metrics
8. Poor educational planning
9. Unmotivated champions
10. Poor social settings
11. High turnover

1. Security Team sets a pace that is not maintainable, and they burn out, drop the ball, and the program unravels.

1. Security Team sets a pace that is not maintainable, and they burn out, drop the ball, and the program unravels.

Solution:

Start slow.

Run only one event per month.

Try to plan out at least 6 months in advance.

Do you have the resources for the program you've designed AND a few security incidents? If not, cut back.

Run it by a trusted colleague or friend.

2. No responsibilities or goals are set out, and the champions have no idea what is expected of them.

No one can achieve an unknown goal.

2. No responsibilities or goals are set out, and the champions have no idea what is expected of them.

No one can achieve an unknown goal.

Solution: Set clear goals and tell everyone.

Examples:

- Provide Sec advice to peers
- Creating and maintaining a more positive security culture on the dev teams
- Threat modelling
- Adding security checkpoints to SDLC

2. No responsibilities or goals are set out, and the champions have no idea what is expected of them.

No one can achieve an unknown goal.

Solution: Set clear goals and tell everyone.

- Triaging scanner results
- Building sec tools and/or sec features
- Liaison between dev and sec teams
- Initiating sec fixes
- Influence and inform security team of what's to come, so they can prepare and adjust

2. No responsibilities or goals are set out, and the champions have no idea what is expected of them.

No one can achieve an unknown goal.

Solution: Set clear goals and tell everyone.

- Helping to implement security tooling or automating it
- Socialize AppSec projects and new tools
- They take Secure Coding training and help others on their team code more securely/review PR requests

3. Champions are forced to volunteer (voluntold), then they underperform and are resentful.

3. Champions are forced to volunteer/voluntold, they underperform and are resentful.

Solution: Attract volunteers instead!

- Let your champs see everything first
- Ask them for feedback and LISTEN to it
- Have events, like lunch and learns and trainings
- Invite them to security community events
- Start a newsletter
- Share (appropriate secrets)

3. Champions are forced to volunteer/voluntold, they underperform and are resentful.

Solution: Attract volunteers instead!

- Send them cool podcast episodes that apply to their work or tech stack
- Meet them 1:1 and ask them what they need help with, then help them
- Hold team building events so they can know each other
- More in next item.


4. Inability to recruit champions.
REE

4. Inability to recruit champions.

Solution: Don't just recruit, attract your champions!

- Hold events to get them in the door
- Make it clear to champions why being a champion is good for THEM, not just why it's good for the sec team.
- Announce you are looking for champs at every opportunity, like an all staff or in a newsletter for your office
- Add it to your email signature
- Arrange security training for all, tell the trainer to help you recruit

4. Inability to recruit champions.

Solution: Don't just recruit, attract your champions!

- Invite people you think might be interested
- Put a sign on the fridge in the kitchen
- Hold open office hours, then tell them about it
- Send an email to all of IT asking (just once, don't be spammy)
- Assure everyone you will teach them all they need to know
- Ask managers if they can think of someone who might be interested

5. Unrealistic Expectations

5. Unrealistic Expectations

The security team expects champions to perform most of the work of the AppSec team or know as much as they do.

This is impossible on top of their regular job and without many years of experience; this expectation is impossible to meet.

5. Unrealistic Expectations

Solution:

- Create realistic expectations for yourselves. Think about what you really need help with, and what the devs can realistically do in the limited time they have.
- Be fair. If the roles were reversed, would you feel your expectations are fair?
- Be very specific. No one likes guessing what is expected of them at work!

6. No support from the top.

6. No support from the top.

Verbal support, financial support, resources, staffing, processes, and policy).

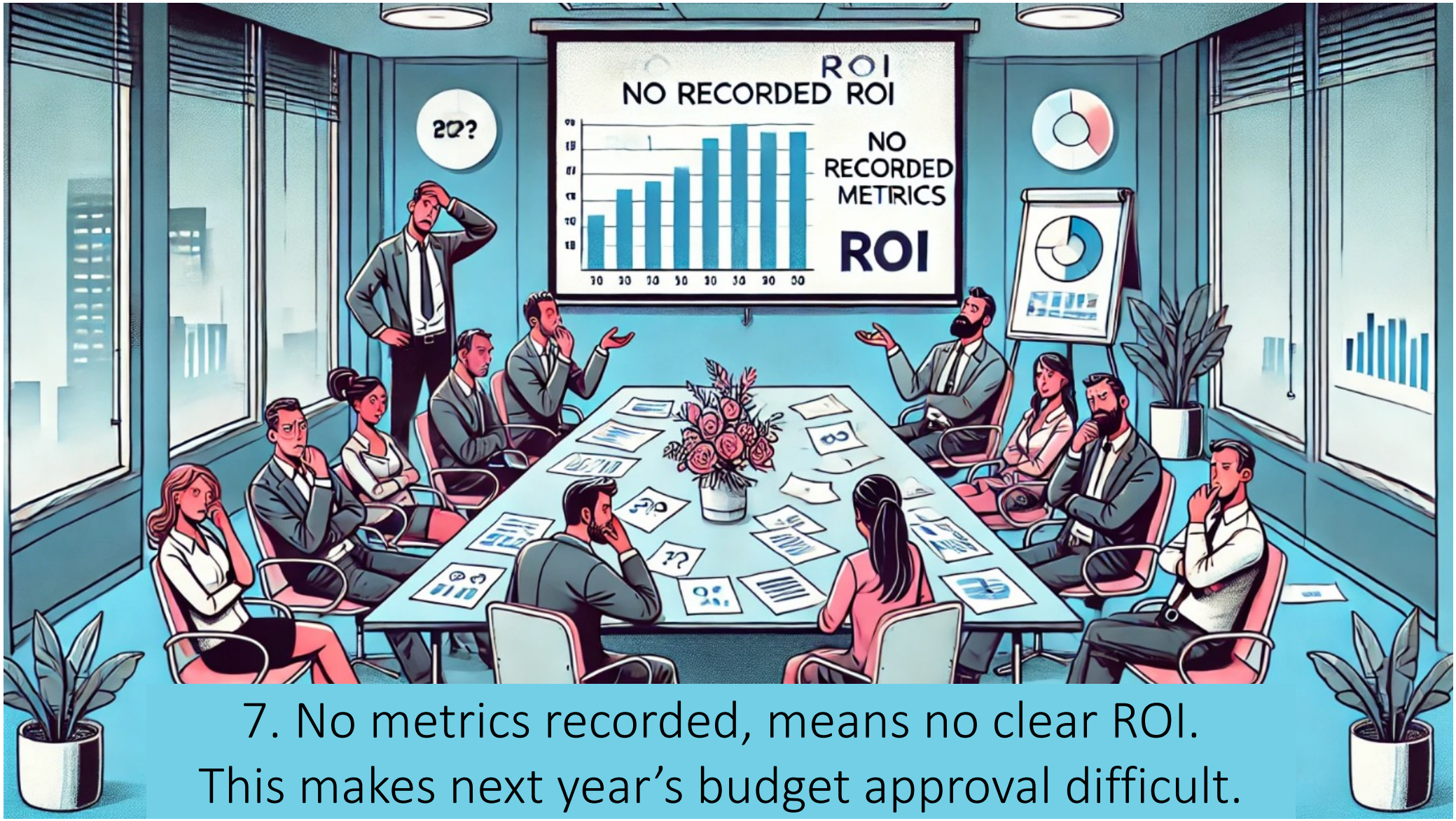
Solution:

- Make a presentation to management to get buy-in
- Create a project plan that is achievable and reasonable

6. No support from the top.

Solution:

- Explain the potential return on investment
- Bring in consultants with previous experience to ENSURE you succeed
- Show examples of other programs that have worked
- Don’t assume people know the value or ROI of a champs program, tell them! Over and over.



7. No metrics recorded, means no clear ROI.
This makes next year’s budget approval difficult.

7. No metrics recorded, means no clear ROI. This makes next year's budget approval difficult.

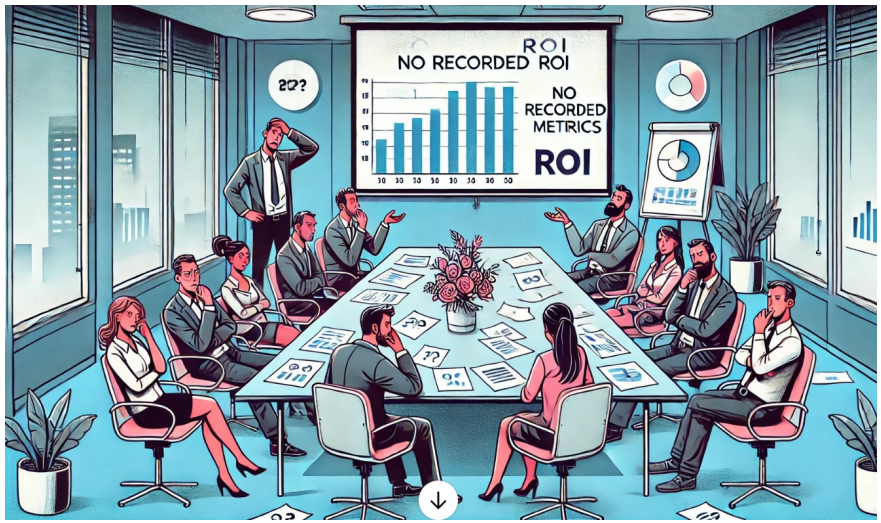
Solution: Take metrics and tell everyone! Especially those senior to you.

- Belt system, each achievement they submit adds to the score, and when they reach a certain score, their belt level increments
- Learning platform, how many lessons they complete
- Participation in events / meeting attendance
- There are SaaS tools that can handle this for you

7. No metrics recorded, means no clear ROI. This makes next year's budget approval difficult.

Solution: Take metrics and tell everyone! Especially those senior to you.

- There were no metrics gathered for over 50% of programs in my surveys
- Champion coverage: How many champions they have per product/app
- Answering security questionnaires
- Phishing instances going down
- Seeming engaged
- Measure your goals
- Measure their responsibilities



8. Poorly planned education.

The Security team doesn’t know what to teach them, and/or runs out of things to do with the champs.

8. Poorly planned education.

Solution:

- Play recordings of really great talks from conferences, then talk about it as a group
- Outsource. Either hire out or ask friends to come present for your team. There are tons of beginner speakers who would love to have a live audience to practice on!
- Bring in trainers.

8. Poorly planned education.

Solution:

- Purchase a security training platform
- Hire a company that runs security champion programs and get them to handle it.
- Ask permission to present the work of others. I have “open sourced” several of my talks, lots of us speakers would be honoured to have someone else present our work, with credit.
- Hire a company to do an AppSec table top exercise

9. Unmotivated Champions

You have lots of champions but they don’t DO anything

9. Unmotivated Champions

Solution:

- Clarify your goals and their responsibilities
- Create a reward system for those who do well
- Eventually replace champions that don’t do well
- Share metrics with them and how their work reduces business risk and even saves the day
- On top of all the engagement items previously covered

10. Poor social settings

Lack of social skills/hosting skills from security team, leads to awkward meetings and interactions

10. Poor social settings

Solution:

- Communication training for the security team
- Bring in consultants that ARE good at this, work with them until you can handle it on your own
- If you have hiring ability, bring in a community manager, even part time. They ROCK at this stuff.
- Realize that no one is perfect. It’s okay if we’re weird sometimes. Just make sure you’re respectful.


10. High turnover
Champions leave after only a short while, meaning security have to start training someone new all over again.
It’s expensive to have constant attrition.

10. High turnover

Solution:

- **Engagement**
- **Make value to champs clear from start**
- **Make expectations clear from start**
- **Ask for feedback regularly so you know if they are losing interest and why.** **(feedback loops)**

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

Since I first created this talk,
I have done more research.

What can go wrong: Updated Research

1. Champions Burnout
2. Loss of interest over time
3. Inceptives aren't tangible
4. No feedback loops
5. Poor Communication
6. Champions not empowered to drive change
7. Micromanagement
8. No roadmap or maturity model
9. Focus only on technical skills
10. Lack of budget
11. Not celebrating wins
12. No succession planning
13. Champions feeling isolated
14. Too much focus on compliance, instead of culture
15. Champions have no tools or resources
16. One-Size-Fits-All approach

Agenda

1. ~~Why Champions?~~
2. ~~What goes wrong and how to do better~~
3. Conclusion

Conclusion

We learned…

1. Champions programs fail if we are not specific and intentional

2. How programs fail and why

3. Several ways to ensure we do not fail

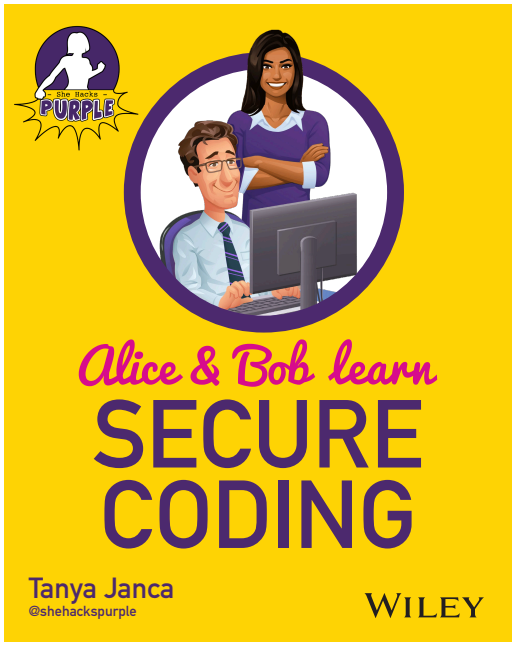
4. How to build an AMAZING program!

OWASP 2025 GLOBAL AppSec | BARCELONA MAY 26-30

Resources

Continue your learning…

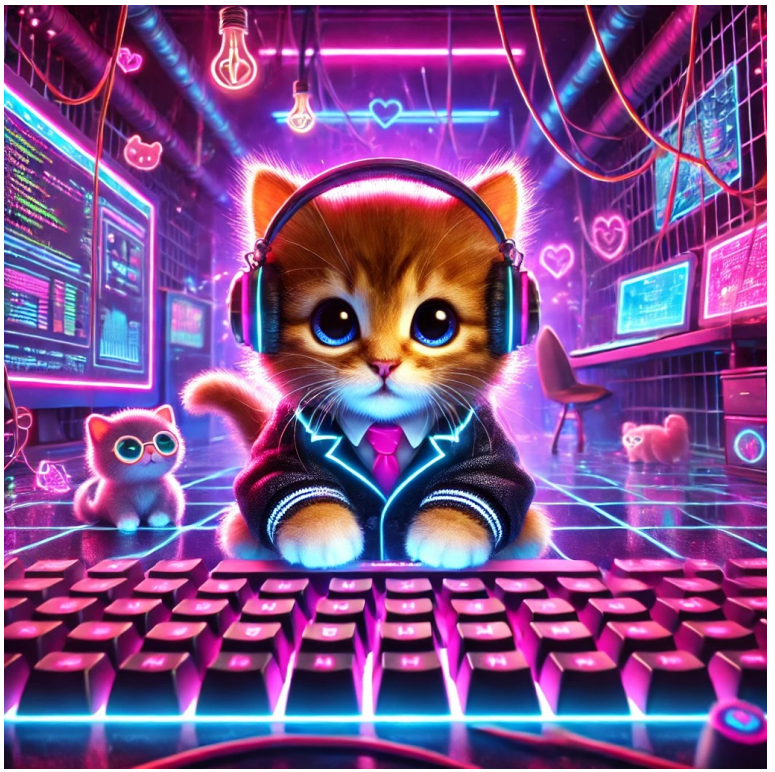
My books!



https://aliceandboblearn.com

My blog series on this topic

https://semgrep.dev/blog/2024/building-security-champions/



Security Champions Success Guide

SecurityChampionSuccessGuide.org

Resources: Meeeeeeeee!

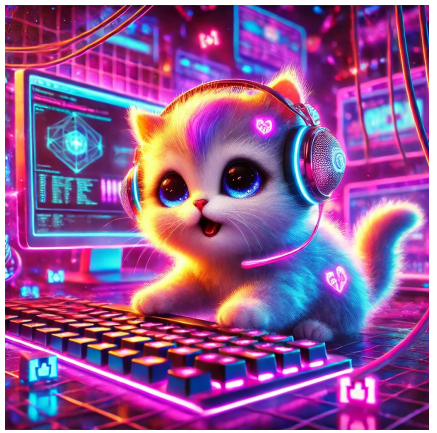
https:// SheHacksPurple.ca

@SheHacksPurple

Twitter/TikTok/Mastodon/GitHub/BlueSky/etc.

https:// SheHacksPurple.ca/blog

https://Newsletter.SheHacksPurple.ca



Mature your AppSec program!

Take the Survey

https://bit.ly/AppSec-Survey


OWASP 2025
GLOBAL
AppSec
BARCELONA
THANK YOU!
Tanya Janca
(SheHacksPurple)