RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PROF-M01**

Transforming Security Champions

Scaling your security!

Tanya Janca

CEO and Founder, We Hack Purple
Director of DevRel and Community, Bright
@SheHacksPurple

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

What are we going to talk about today?

Scaling your security team and program.

What are we going to talk about today?

What security champions are and how to build them up.

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

RSA® Conference2022

Tanya Janca

About ME!

- Director of DevRel and Community at Bright!
- CEO & Founder @ We Hack Purple
- AKA @SheHacksPurple
- Author: **Alice and Bob Learn Application Security**
- 25+ years in tech, Sec + Dev
- Advisor: Nord VPN and Cloud Defense
- Blogger, Podcaster, Streamer, Builder, Breaker
- Nerd at Large

The Problem:

Not enough AppSec Pros.

Scaling Your Team and Program

We know there aren’t enough security professionals to go around.

So we scale.

Photo by Jonathan Borba on Unsplash

Security Champions

A Security Champion is a member of a team that takes on the responsibility of acting as the primary advocate for security within the team and acting as a first line of defense for security issues within the team.

Or more plainly:

The person who is most excited about security on a team. They want to read the book, fix the bug, or ask the security questions. Every time.

What *is* a security champion?

Your communicator

- They deliver security messages to each dev team, teaching, sharing and helping

Your point of contact

- They deliver messages to the security team, and keep you up to date on what matters to your team

Your Advocate

- They perform security work, for their dev team, with your help.
- They also advocate for security.

Let’s *build* security champions!

Recipe; recruit, engage, teach, recognize, reward, don’t stop.

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

Recruiting Your *Champions*

- She Hacks -
PURPLE

Bright Security

#1 Rule in Recruiting

Do not “voluntell” someone to be a security champion.

Attract the right people instead.

#2 Rule in Recruiting

Ensure managers are on board and will give the champs time to do this important work.

Recruit

Ask for volunteers instead of appointing people without consent

Provide opportunities for them to reveal themselves

Add to your email signature that you are looking

Attract volunteers

- Use lunch and learns or trainings
- Anyone who asks questions or attends all the events is a potential champion
- Use interesting titles for events if you can

Your new mantra will get you results: “It’s my job to serve you”

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

RSA® Conference2022

Engage your champions

Occupy, attract, involve – in security activities

Participate or become involved – with your champs!

Engage:

- bring them on an incident,
- share (appropriate) secrets, Deputizing and sharing sensitive info
- Let them see everything first, new tools, changes, information, etc.
- Create a mailing list to tell them new security stuff

Engage:

- Meet with them once every month, and have a present list of questions
- Brace yourself for bad news so that you can play it cool
- Team building events, let them know each other
- Invite them to join security communities

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

RSAConference2022

What are you going to teach your champs?

Bright

Only what they need to know.
Nothing more.

What you need, expect and want from them, as champions.

Topics for Champions!

Secure Coding and Architecture

Your policies

Tooling!

Secure Coding and Architecture

Topics for Champions!

- Formal training on secure coding, with labs!
- Threat modelling
- Secure architecture (whiteboarding)
- Code Review
- How to fix the bugs they find
- Repeat yearly as a minimum

Your Policies

Topics for Champions!

- Which policies, standards and guidelines apply to them
- Help them create missing guidelines
- Teach them how to be compliant, help them get there
- Their role during an incident
- Job shadowing
- Hold consultations to let them provide input on the policies that will affect them

Tooling

Topics for Champions!

- Custom training on tools they use
- What the output means
- How to validate results of tools
- How to install and configure tools
- Help them select the BEST tools
- Lunch and learns or hack-a-thons

Coaching

(a style of Teaching)

Coaching

Coaching means enabling individuals and teams to achieve their full potential.

Facilitating the exploration of needs, motivations, skills and processes to assist them in making real, lasting change.

If we want teams to start practicing a *secure* SDLC, we need to support them getting there.

If we want security champions, we need to constantly reinforce the values we want them to evangelize.

Coaching

For Champions:

- Set up office hours
- Set repeating meetings
- Help them prioritize their security activities or bugs
- Always **be available**
- Help them set goals, then achieve them
- Teach them specific skills or tools
- Ask them what they need, then provide

A special note on Delegation

Some items shouldn’t be the responsibility of the AppSec team, even if you know how.

- Fixing security bugs
- Updating frameworks
- Planning releases or upgrades
- Assignment of bugs to developers
- Running every scan
- Implementing and/or tuning every tool
- Writing unit tests

The list is endless, delegate what makes sense.

Do Not Delegate

Some items shouldn't be delegated.

- Validating SAST results
- Giving security's approval on new technologies (or anything else on behalf of your team)
- Using new tools without proper training
- Training new champions

We are looking for partnership and assistance, not replacements for our team.

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

RSA® Conference2022

It’s important to recognize your champions.

We want them to know they are doing a good job, and not feel like the are trying really hard to do two jobs, for one paycheck.

Recognize:

- Create a Certificate to put on their wall,
- Recognize them in front of their peers (special virtual background, star on their name is slack, etc.)
- Make sure to put a note in their performance review

Recognize:

- Tell their boss every time they do something that makes a big difference
- Send them an email and tell them when they did something big, let them know that YOU saw
- Make their role on their team clear to them and their peers

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

RSA Conference2022

Reward them!

Reinforce good behavior, instead of punishing bad.

Reward good behaviour with anything you (reasonably) can.

- Security-related gifts - books, videos, training, CTFs.
- Giving them your time and attention is a reward.
- Help them with more than just security.
- Let them see a new tool first.
- Let them help you make decisions.
- Anything else you can think of.

What is the recipe we will follow?

1. Recruit
2. Engage
3. Teach
4. Recognize
5. Reward
6. Don’t Stop!

RSA® Conference2022

When in doubt, overcommunicate.

If you do not communicate regularly, your program will disappear.

Quickly.

Don’t let it slip

- Consistency is key
- Even if you just meet with them once a
  with them
- Some cham of your time than others,
  orm better than others
- u have accidentally ‘dropped’ your schedule, pick it back
  as as soon as possible
- Culture is a practice, it must be repeated over and over

It will fall apart faster than you think.

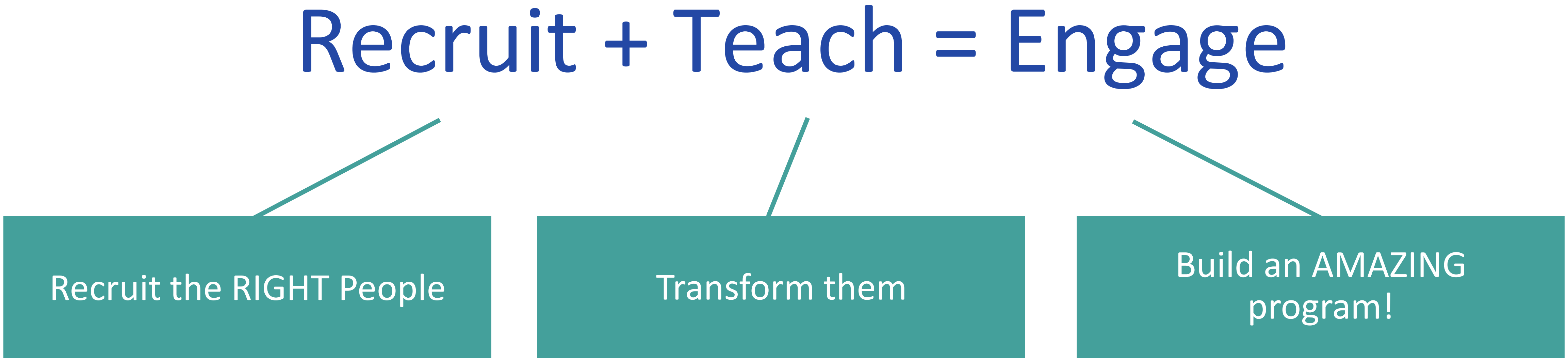
What is the recipe we will follow?

1. Recruit
2. Engage
3. Tea
4 gnize
5. Reward
6. Don’t Stop!

We did it!

Conference2022

Apply What You Learned!



Recruit + Teach = Engage

Recruit the RIGHT People

Transform them

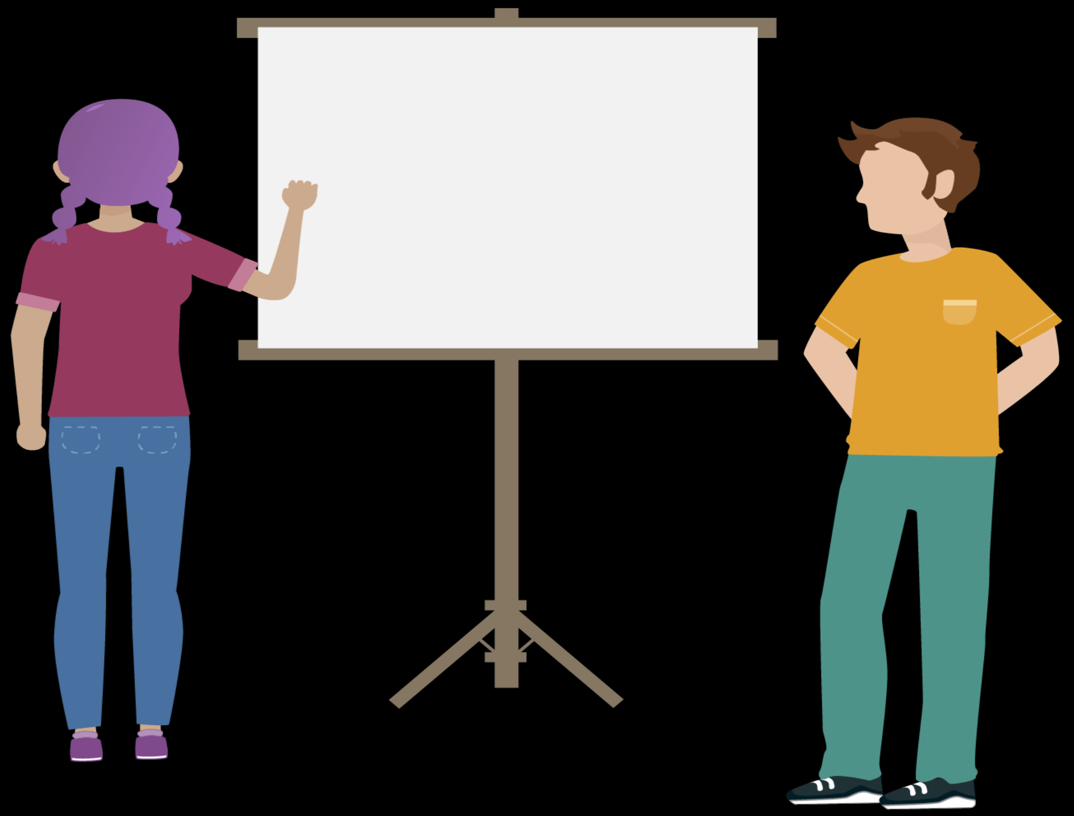
Build an AMAZING program!

Most Importantly: DO NOT STOP!

Apply What You Have Learned Today

- Next week you should:
  - Start Recruiting New Champions, Create a List of Goals
- In the first three months following this presentation you should:
  - Have 3 lunch and learns, and monthly meetings
  - Teach them at least one of the things you need them to know
- Within six months you should:
  - Do at least one ‘Reward’ and one ‘Recognition’ activity
  - Continue monthly 1:1 meetings and lunch and learn events
  - Check your metrics!

Resources



Bright Security

Awesome Books

- The DevOps Handbook
- The Phoenix Project
- Accelerate
- The Unicorn Project
- Alice and Bob Learn Application Security

Join the community!!!!!

Join the We Hack Purple Community for FREE

Community.WeHackPurple.com

Meet like-minded people and nerd out!

I have a podcast!!!!!

We Hack Purple Podcast, season 2, offers all sorts of security advice and best practices! Watch it on YouTube or subscribe on any platform.

https://www.youtube.com/WeHackPurple

Resources: Meeeeeeeee!

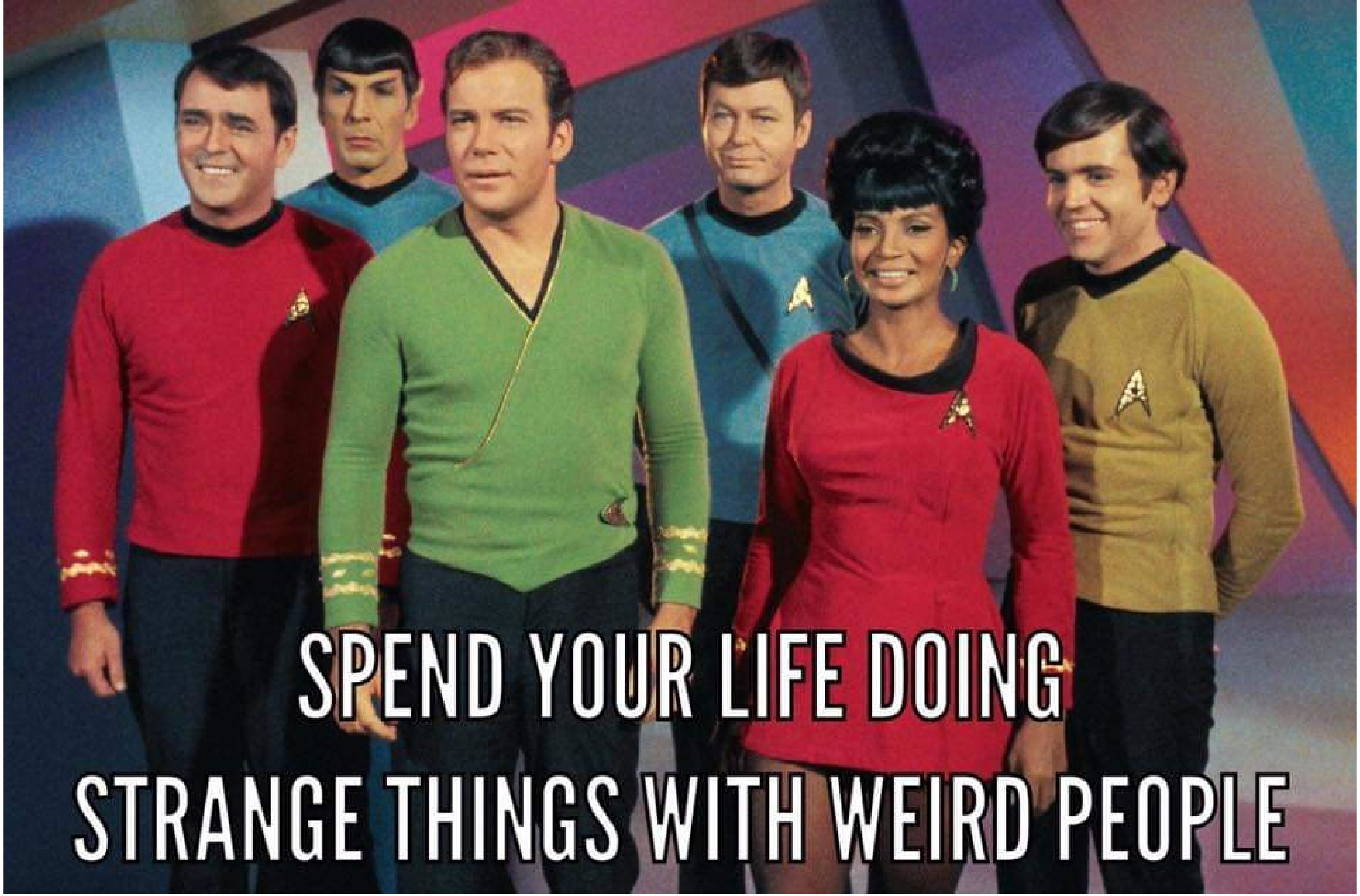
@SheHacksPurple

YouTube.com/SheHacksPurple

https://WeHackPurple.com/blogs

https:// SheHacksPurple.ca/blog

https://Newsletter.SheHacksPurple.ca


SPEND YOUR LIFE DOING
STRANGE THINGS WITH WEIRD PEOPLE

THANK YOU!

Tanya Janca

DevRel @ Bright

We Hack Purple