OWASP
Open Web Application
Security Project

Security Champions 2.0

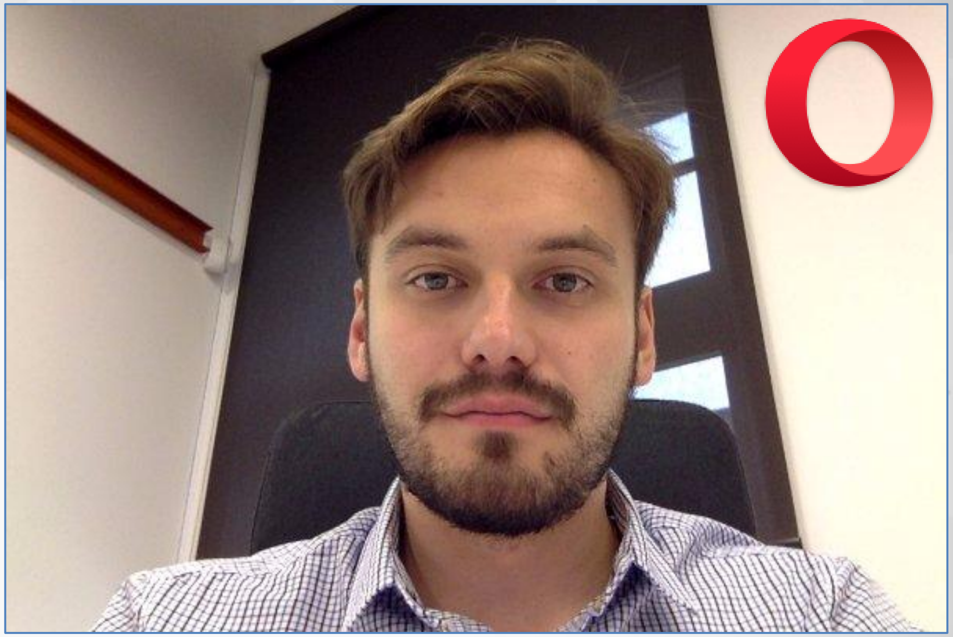
OWASP Bucharest AppSec 2017

Alexander Antukh

Whoami

- Head of Appsec
- Opera Software

- @c0rdis



Champions, really?

Previous works

Nice presentation
“Security champions v1.0”

“New era of software with
modern appsec”

Imagine *theoretical* situation

- Many projects
- Even more teams
- Different technologies
- No strong security culture

VS

YOU

What is a security culture?

- Open-mindness?
- Personal engagement?
- Responsibility?
- Knowledge sharing?
- Management support?

“Security is important! But…”

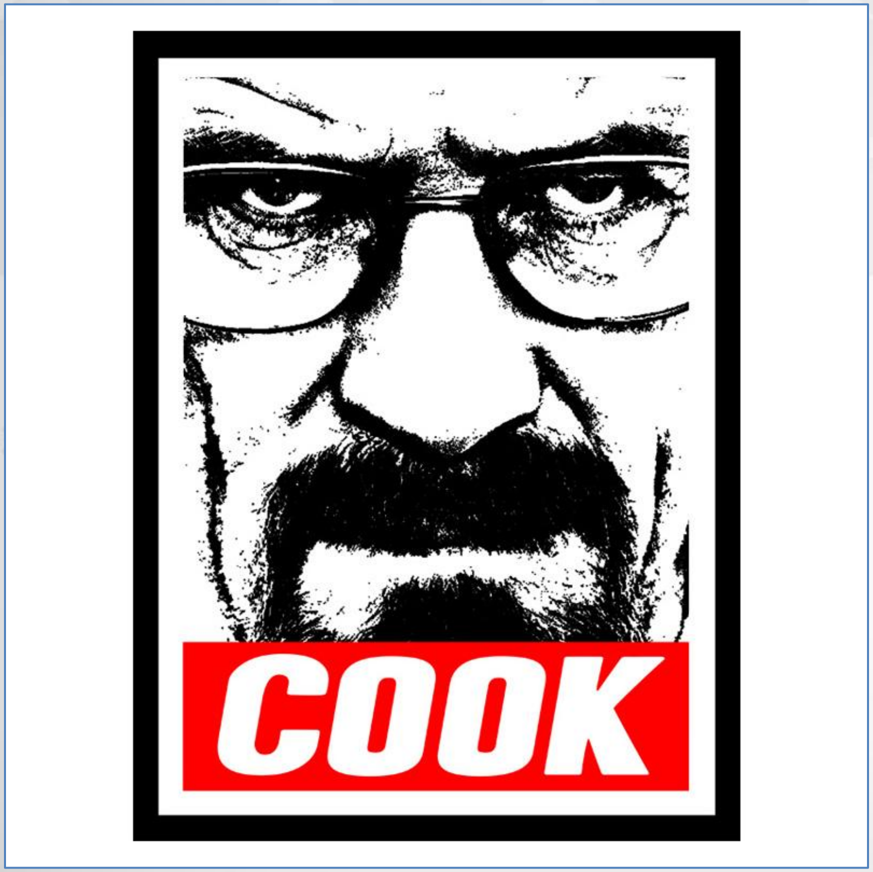
- … it’s good enough for now
- … these risks are not relevant
- … it’s just a pilot project
- … we’re changing too fast
- … we depend on third-party solutions
- … we don’t want no formalisms

So what's with the Champions?

Security Champions

- Developers
- QAs
- Architects
- Designers
- DevOps
- Anyone interested!

Security Champion is …

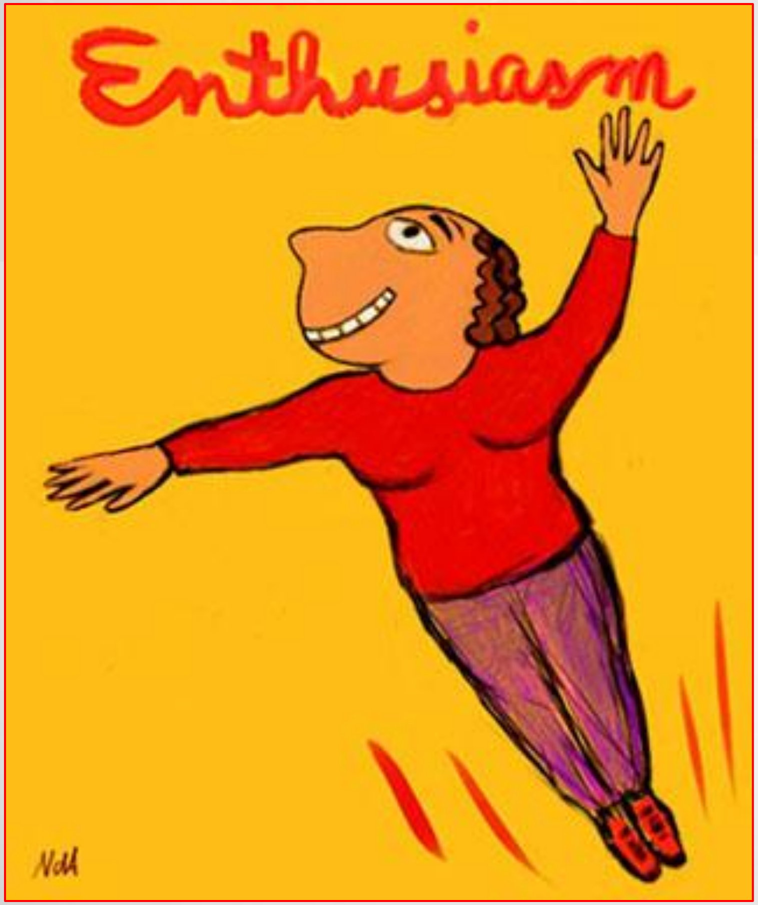


someone with an insight to the project internal kitchen

Security Champion is …

someone who becomes the team’s security SPOC

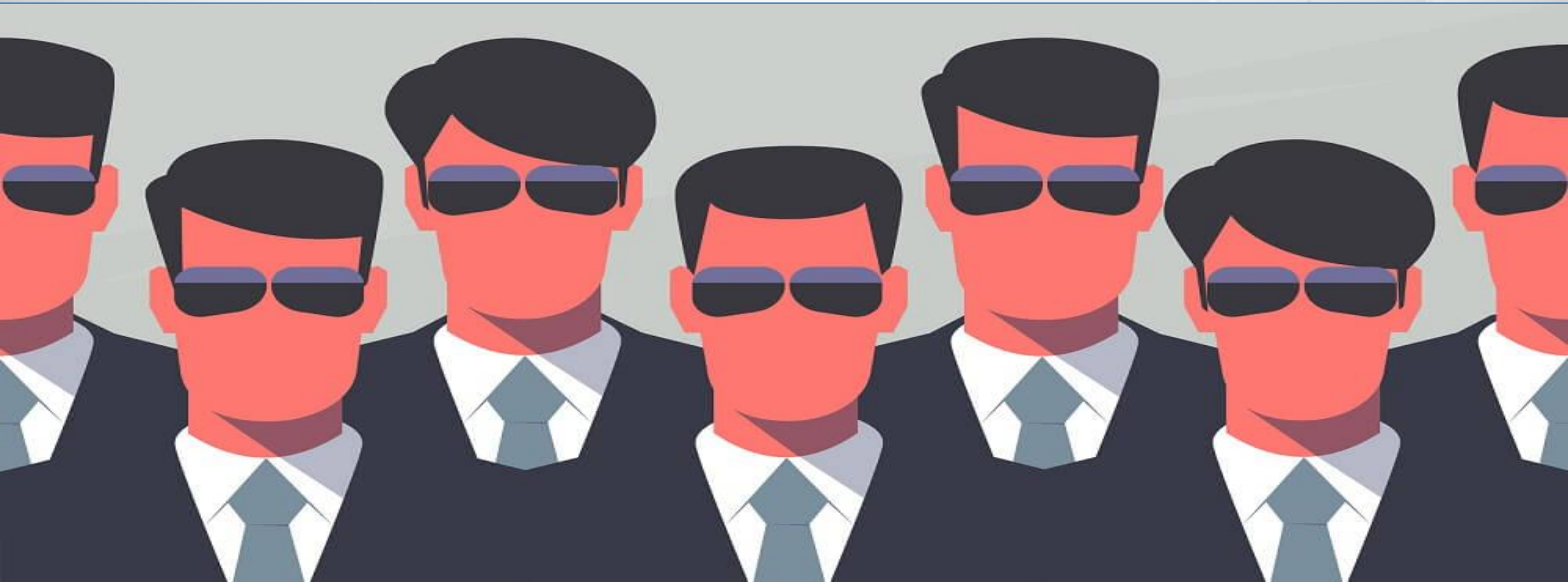
But what's more important, it's…



someone who wants to upgrade security

Benefits of having sec champs

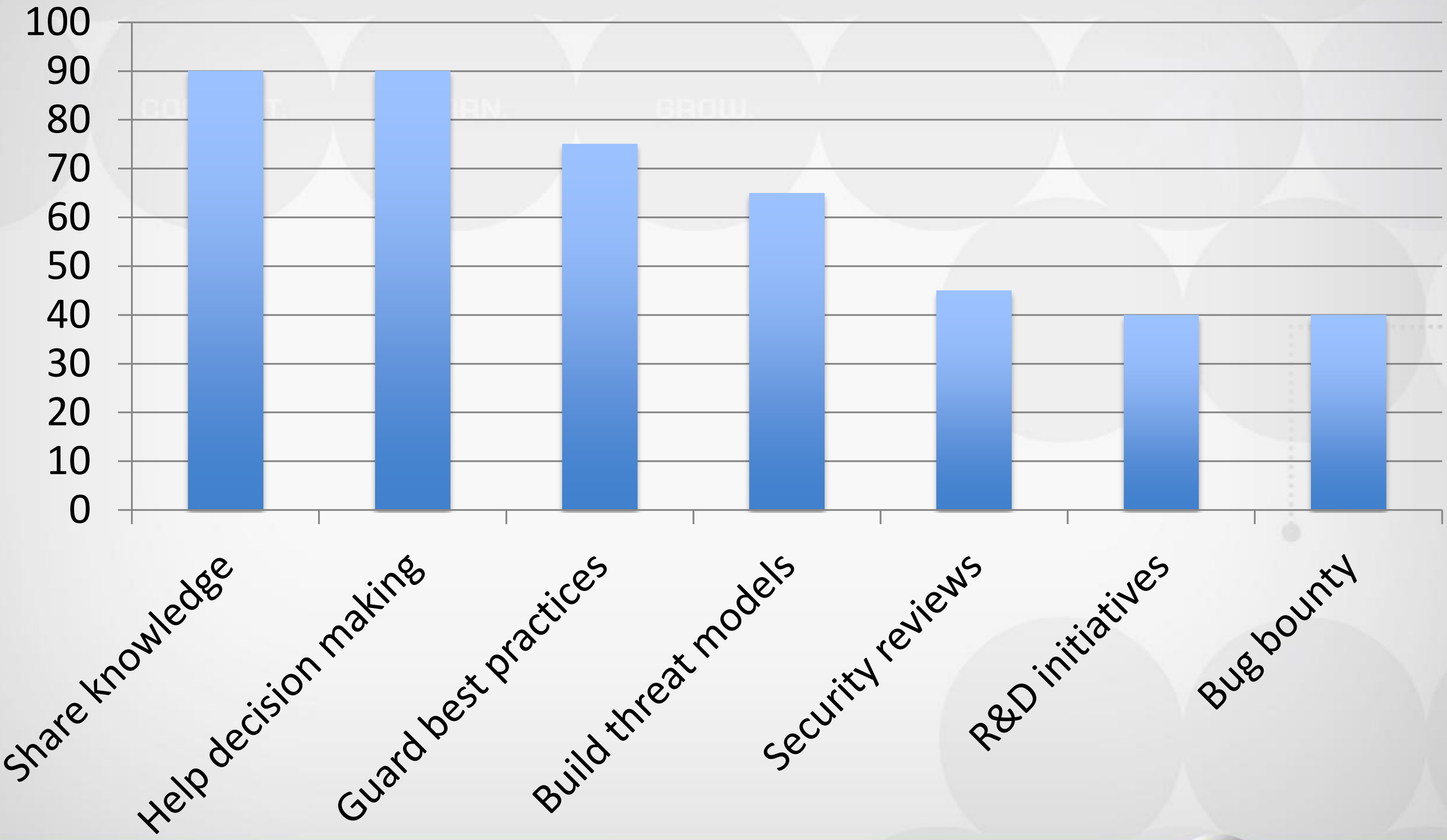
- Scaling security through multiple teams
- Engaging “non-security” folks
- ***Creating a security culture***



Security Champions at OWASP SUMMIT 2017

- Security Champion survey
- 11 questions, 7 yes/no + proposals/ideas
- 20 respondents
  - – CISOs
  - – project leaders
  - – developers
  - – testers
  - – architects

Security Champion expectations



Other selected expectations

- Attend security conferences
- Define best practices
- Prioritize security-relevant stories in Backlog
- Monitor vulnerabilities in tools/libraries
- Write security tests for identified risks

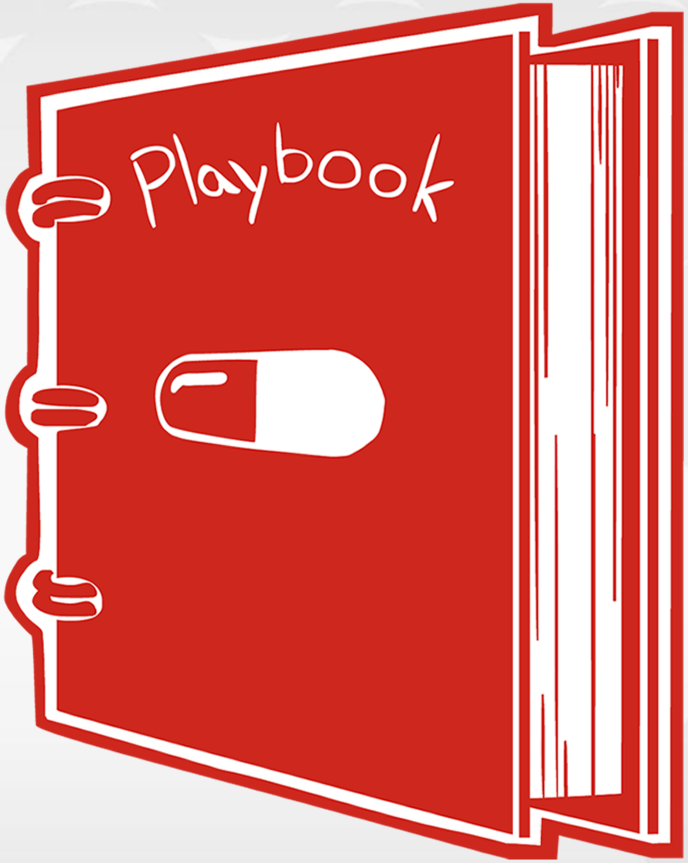
More outcomes: http://bit.do/security_champions

So far it looks like that:

- You’re alone with a million of security problems
- ?????
- Champions appear and solve them

PROFIT!

Security Champions Playbook



Security Champions Playbook

1. Identify the teams
2. Define the role
3. *Nominate* champions
4. Set up communication channels
5. Build solid knowledge base
6. Maintain interest

1. Identify the teams

- 1 product = 1 team?
- Technologies?
- Documentation?
- Communication?
- Management?
- Current reviews?
- Release calendar?

1. Identify the teams

Expected outcome after this step:

Product	Team	Technologies	Security contact	Team lead	Product manager	BTS	Comments
Product1	Alpha	Python, Django	John Smith	John Smith	Anna Nowak	HELO	Usage of Bandit tool
Product1	Beta	…	…	…	…	…	…

2. Define the role

- Measure current security state among the teams
- Define goals you plan to achieve in mid-term
- Identify places where Champions could help
- Produce clearly defined roles for the Champions

OPENSAMM

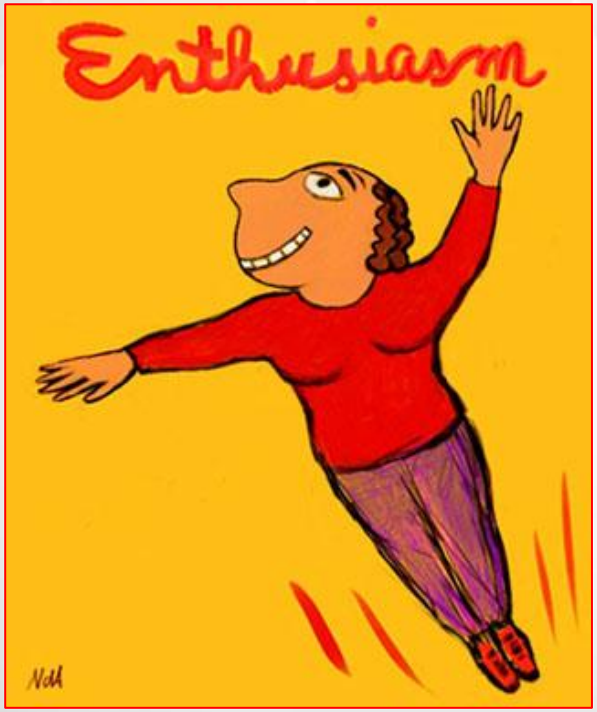
2. Define the role

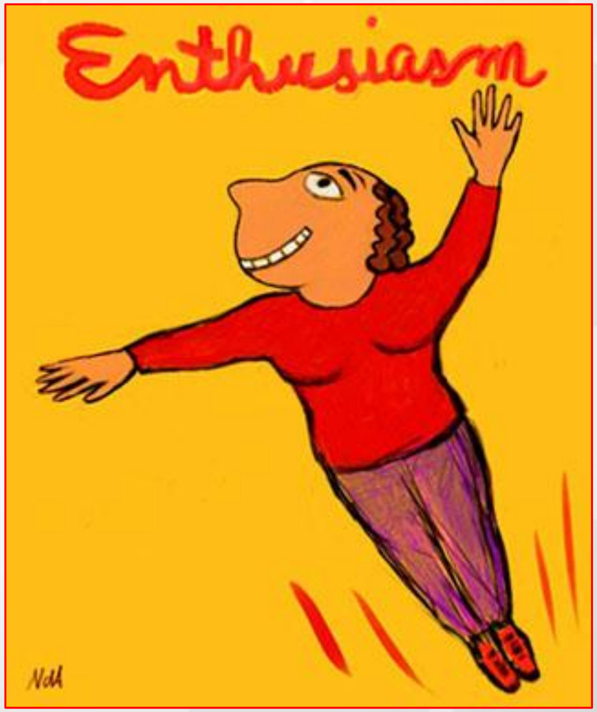
Depending on current progress and strategy, roles descriptions could be:

- Verify security reviews
- Control best practices within the team
- Raise issues for risks in the existing code
- Build threat models for new features
- Conduct automated scans for the code
- Investigate bug bounty reports

3. *Nominate* Champions

- Not appoint!! Enthusiasm, remember? ;)



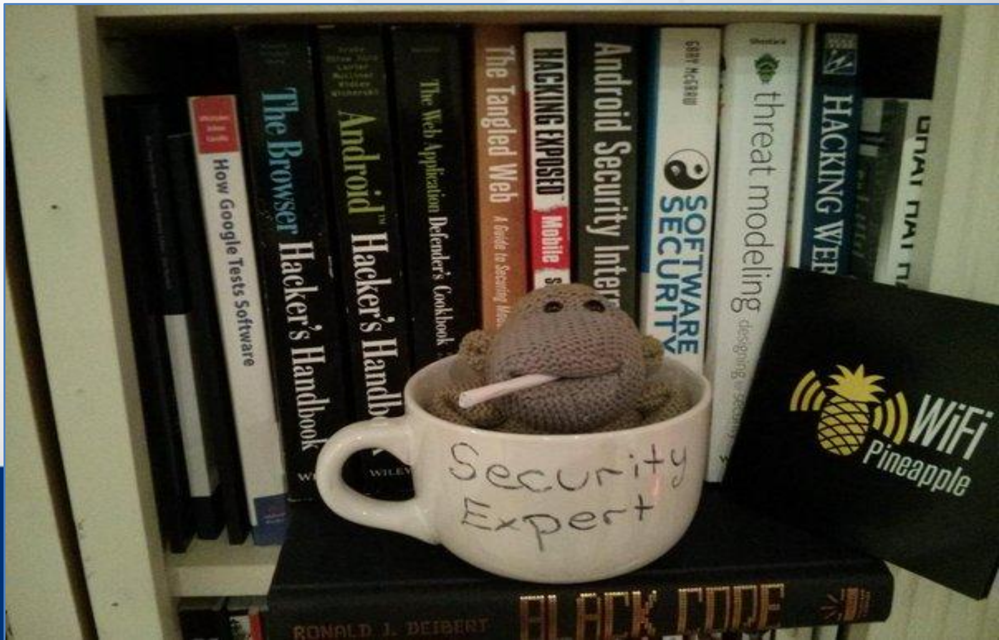


3. *Nominate* Champions

- Get approvals on all levels
- …
- Because otherwise you'll hear the worst argument ever
- **I HAD NO TIME FOR SECURITY!!!**

3. *Nominate* Champions

- Once nominated, make him feel like a Champion:
  - – entry to the security meta-team
  - – official introduction to the peers
  - – insignia ;)


How Google Tests Software
The Browser Hacker's Handbook
Android Hacker's Handbook
The Web Application Defender's Cookbook
The Tangled Web
HACKING EXPOSED Mobile
Android Security Internals
SOFTWARE SECURITY
threat modeling
HACKING WEB
Security Expert
WiFi Pineapple
BLACK CODE
RONALD J. DEIBERT

4. Set up communication channels

- Slack?
- IRC?
- Skype?
- Keybase?
- Yammer?
- Mailing lists?

5. Build solid knowledge base

Internal wiki as the main source

- Security meta-team with listed champs
- Clearly defined roles and procedures
- Secure development best practices
- Risks & vulnerabilities
- **Checklists** →

✓ Web/mobile security checklist
✓ Third-party security checklist
✓ UI security checklist
✓ Privacy checklist
✓ …

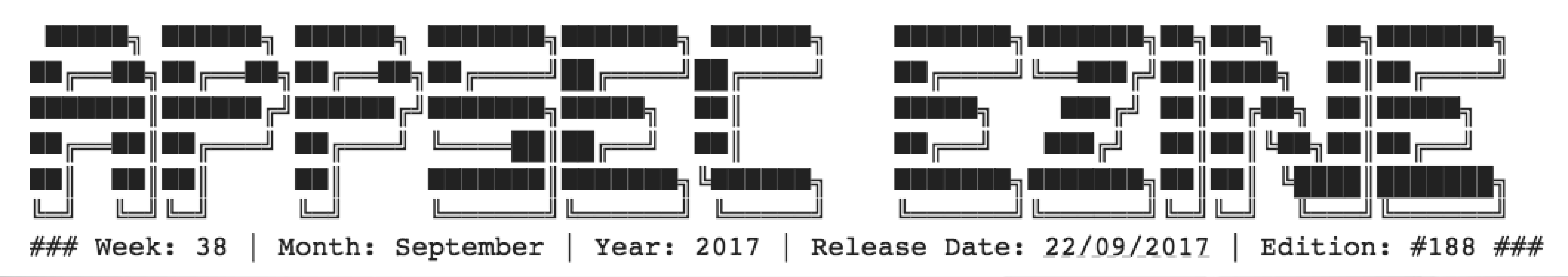
5. Build solid knowledge base

- Open source to the rescue!
  - Security Knowledge Framework
  - ASVS + MASVS
  - CERT secure coding standards
  - and many more…

6. Maintain interest

- Workshops & trainings
  - Strategy / best practices
  - Security quizes
  - Hacker Thursdays
  - ["Month of bugs”]
- Keep them motivated!

6. Maintain interest



APPSEC EZINE

Week: 38 | Month: September | Year: 2017 | Release Date: 22/09/2017 | Edition: #188

- https://github.com/Simpsonpt/AppSecEzine
- https://github.com/paragonie/awesome-appsec

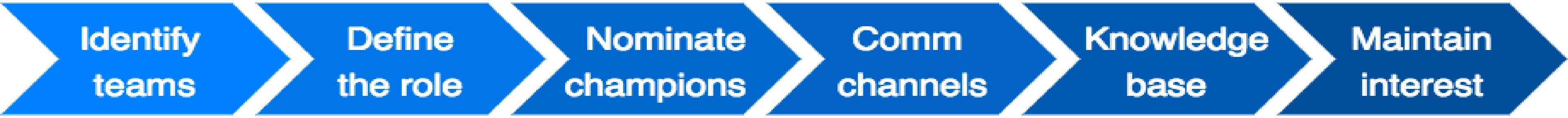
6. Maintain interest

- Monthly security newsletters
  - Updates & plans
  - Recognition for leaders
  - Another source of communication
  - Also serve as checkpoints for all

6. Maintain interest

- Security conference calendar
  - Start here: https://infosec-conferences.com
  - Add your local events…
  - And help to organize OWASP Chapter meetings! ☺

Security Champions playbook



Identify teams

- Enumerate products and services
- List teams per each product
- Identify Product manager (responsible for product) and team manager (working directly with developers)
- Write down technologies (programming languages) used by each team

Define the role

- Measure current security state among the teams and define security goals you plan to achieve in mid-term (e.g. by using OWASP SAMM)
- Identify the places where champions could help (such as verifying security reviews, raising issues for risks in existing code, conducting automated scans etc.)
- Write down clearly defined roles, as these will be the primary tasks for newly nominated champions to work on

Nominate champions

- Introduce the idea and role descriptions and get approvals on all levels - both from product and engineering managers, as well as from top management
- Together with team leader identify potentially interested candidates
- Officially nominate them as part of your security meta-team

Comm channels

- Make sure to have an easy way to spread information and get feedback
- While differing from company to company, this usually includes chats (Slack/IRC channel, Yammer group, ...) and separate mailing lists
- Set up periodic sync ups - bi-weekly should be fine to start with

Knowledge base

- Build a solid internal security knowledge base, which would become the main source of inspiration for the champions
- It should include security meta-team page with defined roles, secure development best practices, descriptions of risks and vulnerabilities and any other relevant info
- Pay special attention to clear and easy-to-follow checklists, as it's usually the simplest way to get the things going

Maintain interest

- Develop your ways or choose one of the below to keep in touch and maintain the interest of the champions
- Conduct periodic workshops and encourage participation in security conferences
- Share recent appsec news (e.g. Ezine) via communication channels
- Send internal monthly security newsletters with updates, plans and recognitions for the good work
- Create champions corner with security library, conference calendar, and other interesting materials

https://github.com/c0rdis/security-champions-playbook

OWASP
Open Web Application Security Project

Afterword

- The playbook will allow you to get sec reinforcements but **THINK BIGGER!**
- Once established properly, they will greatly help you in spreading security across the company and in achieving future sec goals
- … and the best is to see how *they* develop themselves!

Questions?

@c0rdis