CULTIVATING CYBERSECURITY:

BUILDING AND SUSTAINING A SECURITY CHAMPIONS PROGRAM

WHO AM I

Jay Simmons

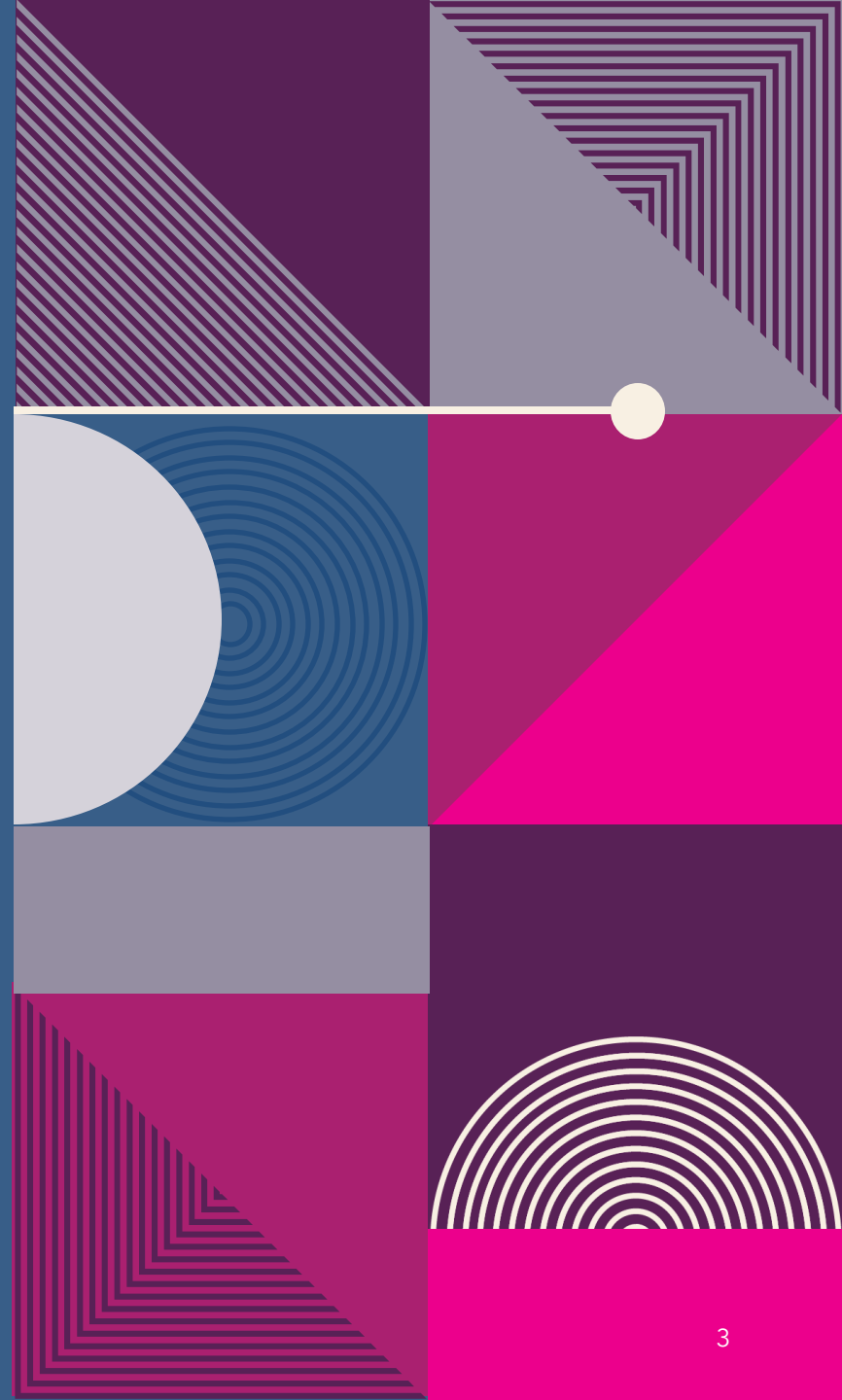
- AppSec Analyst @ Great American
- Owner / Consultant @ Robotti Tech Services
- Information Technology Enthusiast
- Fan of comedy television without laugh tracks.

// Oddly specific but okay.

//Unconventional

MY ENTRY INTO APPSEC

- Started in sales *// Circuit-City if anybody remembers.*
- Did some helpdesk roles *// Paradigm Shift*
- Break Fix / Configuration / Provisioning *// Pomeroy*
- Network & Server/System Administration *// Datacenter*
- Desktop Support *// Lots of helping people and ownership*
- Software Development



AFTER TRAINING

// Why it's more than just training.

```
<h1>
  <%- getGreeting() %>
</h1>
```


```
var name = `<script>
  alert('PWND')
</script>`;
function getGreeting(){
  return `Hello ${name}`;
}
```

SO, WHAT DO WE DO?

Why do we need security champions?

Security Champions

Security champions programs have long been an enabler for software security teams. A security champion is usually a developer, QA tester, or architect who is deputized into an enabler role and provided with additional training and security resources to be the local security professional in a development team. BSIMM14 firms with a security champions program (80 of 130 firms) score on average 25% higher (13 observed activities) than firms without one (50 of 130). This aspect of shared responsibility is crucial to scaling distributed security tasks such as tool automation, security defect triage and remediation, and incident response. Additionally, in BSIMM14, programs with security champions had several training activities that were present at a much higher rate than those without. These training activities include *conduct software security awareness training* and *deliver on-demand individual training*, which were about 40% and 50% higher in firms with champions than those without, as well as *include security resources in onboarding*, which was 33% higher. Having trained security champions and developers facilitates smarter tool use and more secure development.

BSIMM14 Report

- **Security champions (satellite).** Very few SSGs can become large enough to do their business-as-usual tasks and also be responsive to all stakeholders all the time. A security champions group is an effective way to scale SSG reach by embedding trained experts in stakeholder business processes. Security champions take on tasks such as running security tools and doing testing results triage, on-demand training, research on complicated security issues, and ensuring that software security checkpoints are passed successfully.

Some important terms:

- SSG – Software Security Group *(AppSec Team)*
- Satellite – Security Champion

AFTER TRAINING

// Why it's more than just training.

```
<h1>
  <%- getGreeting() %>
</h1>
```


```
var name = `<script>
  alert('PWND')
</script>`;
function getGreeting(){
  return `Hello ${name}`;
}
```

BUT IT'S NOT EASY.

The complexity of a security champion program

OWASP Security Champions Guide

CULTURE MATTERS

Like really, really matters!

THE DEVELOPER CULTURE

I want to build a thing that is super awesome, and everybody wants to use.

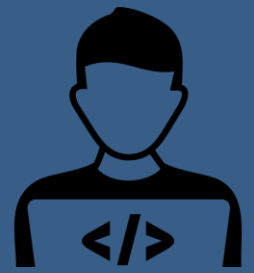
I build a thing that is super awesome and learn a lot in the process.

I show the thing I built to my team, and it becomes a must have core component for our group.

THE SECURITY CULTURE

I want to find a thing that is super broken and get it fixed so I can save the day.

I find a thing that is super broken and learn a lot in the process.



I show the broken thing I found and all the ways it's broken to my group and the people who made the thing. The thing gets fixed and I save the day!

DO YOU SEE THE PROBLEM?

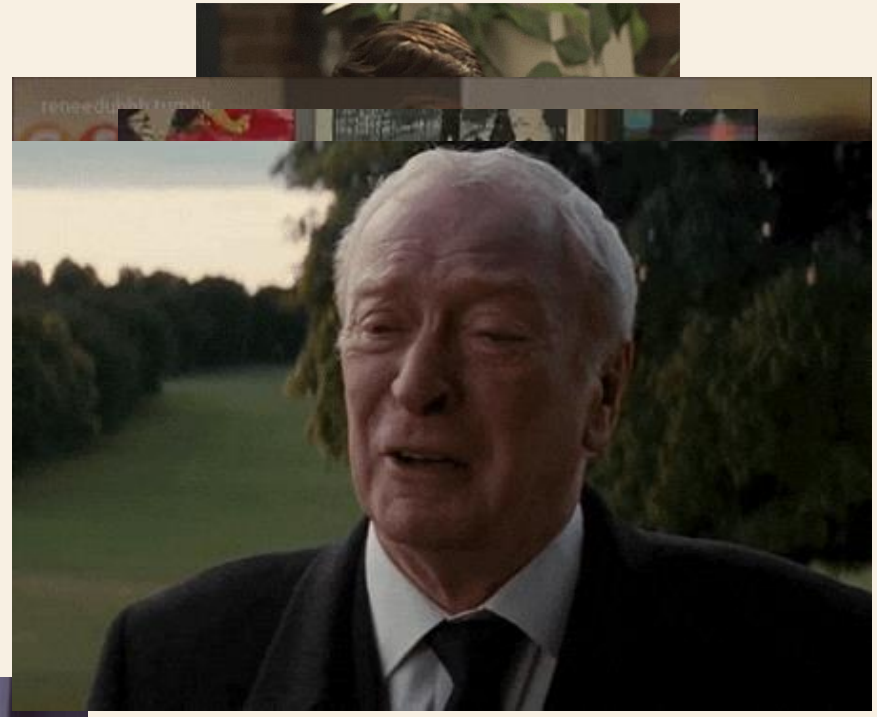
HOW DO WE FIX IT?

Building a security champions program

"JUST CULTURE"
WE NEED TRUST & UNDERSTANDING

Example Scenario

- An XSS finding is discovered in a major web application.
- A developer lets it slip that other people on his team have an app to auto approve MFA requests.
- During an architecture review a developer shows you a database that has unencrypted passwords stored in it.



APPSEC CULTURE

To get developers to:	**Security Groups need to:**
Write Secure Code	Assist & Educate developers
Understand security concerns	Communicate the why of security concerns with examples
Trust our security group	Provide a safe space for solutioning rather than finger pointing
Focus effort on security defects	Acquire top down buy in from leadership & management

BE THE COOL CLUB

Maintaining & Growing the Program

Do this:

- Communicate & Share
- Enable & Encourage
- Recognize & Reward

Don’t do this:

- Voluntell & Enlist
- Slow & Shame
- Ignore their wins

BEFORE & AFTER

Before we would:	**Now we:**
Ask managers to identify security champions.	Identify potential champions from word of mouth & developer meetings.
Prescribe fixes & mitigations for issues.	Collaborate on fixes & mitigations.
Assign workloads and expect them to be completed.	Discuss the problems and work together to prioritize the resolutions.
Expect developers to only focus on development	Educate developers on how we identified the findings & AppSec best practices.

TIPS & TAKEAWAYS

Listen to your champions

- Ask them questions, collect their feedback, and action on it.

Inspire & Enable your champions

- Get their feedback.
- Work together to make big changes.
- Let them be a part of the resolution, not just the problem.

Shift the narrative

- From “Who did this?” to “How can we do better?”

Make the program a “Win-Win” situation.

- Identify ways to get resolution for all stakeholders

1. Seek feedback
2. Reflect on performance
3. Explore new techniques
4. Communicate program goals & progress
5. Iterate and adapt

THANK YOU

Jay Simmons

j.simmons@owasp.org

Robotti.io