Let's Talk About Security Champions

Darylynn Ross
Jay Bobo

Who we are

What we are not talking about

What we are talking about

Please don't hold questions to the end

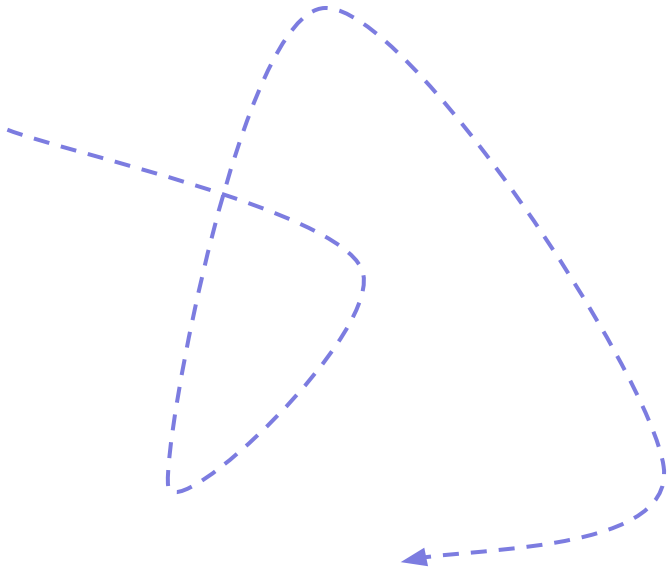
Discussion is encouraged!

History:

Where We Came From

Startup Phase

- Strong training culture
- 30% YoY growth
- (1) app sec engineer
- 150+ apps (25% external)
- Loads of sensitive data



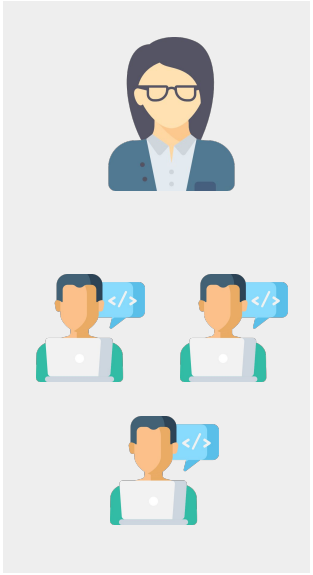
We discovered that...

Early Problems

1. No transparency
2. Developers lacked context
   a. Risk management 101
   b. Cost of a breach
   c. No feedback loops
   d. Lack of control
3. Product leadership was unaware

"I don't control what gets worked on each sprint."

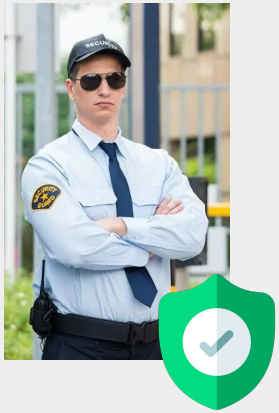
“We don’t have time to do security because...”



Engineering

Product Leadership

“We decide what gets worked on and when, but...”



“What are your biggest technical risks?”

“No clue.”

Lightbulb Moment

Probability of revenue loss

Security

“Impacts to product revenue???”

“How can we help?”

Senior Leaders

Product Leadership

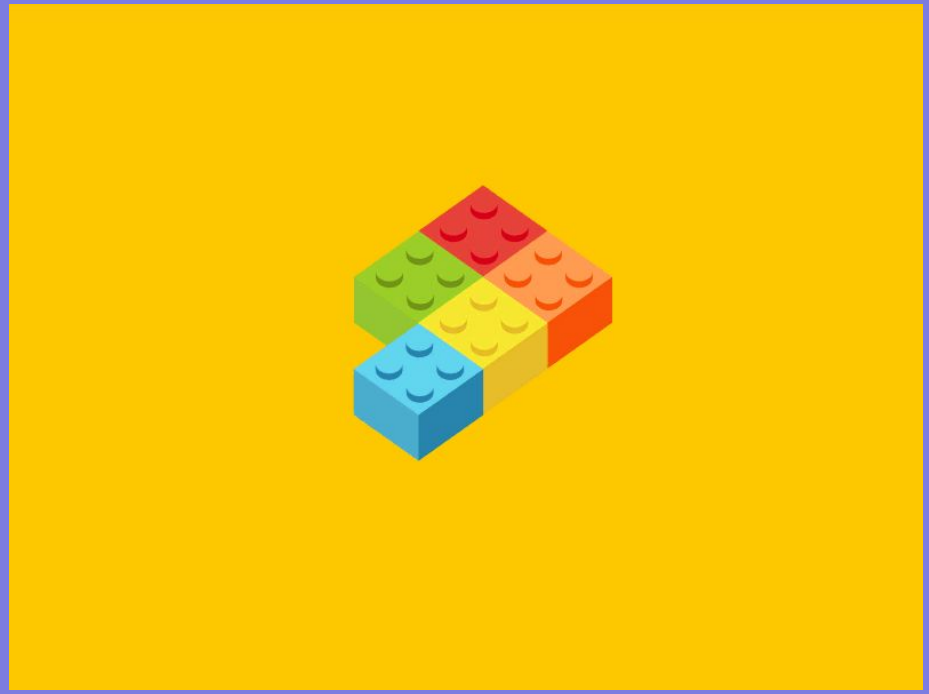
Engineering Directors

Security

Security Champions

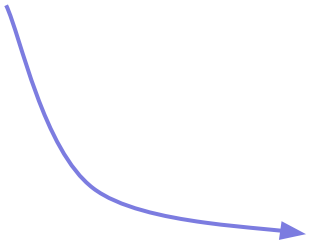
History:

What It Took To Build



Early Champion Group

- One champion per product vertical
- Points of contact for security
- Quarterly state of security report
- Has decision-making authority
- Meets monthly



BSIMM

NIST

OWASP®

Closing the loop

The team that builds the product also…

- Participates in risk analyses
- Enabled to implement security tools
- Has access to the data
- Participates in creation of security standards and guidelines

Security Community of Practice (Security CoP)

Created by Jay Bobo, last modified on Oct 02, 2019

Sponsored by:

ITGRC & SecOps

Contents:

When/Where:

How to Receive Invites:

Add yourself to our distribution list on Outlook or

Contact Us:

(Slack)

Security Working Group:

See description & responsibilities under About Us:

About Us

Our vision is to develop strong security standards for our products and platform, focused training efforts to raise staff ability, and to aid CoverMyMeds in advancing cross-vertical security issues.

Our mission is risk mitigation and improved security through communication, shared knowledge and experience, and best-fit practices and standards.

We are composed of **two bodies**:

- The Security Community of Practice
- Security Working Group

What's the difference between the SCoP and SWG?

› Learn more here...

What We're Working On:

- Pharmacy - Security Tasks and Priorities
- Customer Operations - Security
- Pharma - Application Upgrades
- Provider - Refined Work
- Payer - Security
- Patient - tbd
- Specialty - Security

Our FY2020 Priorities:

Each security working group member representing their vertical selected the following company-wide priorities. We will report back quarterly to our Engineering Directors on the progress made: FY20 Security Priorities

FY2020 Q1 State of Security Report

Created by Jay Bobo, last modified on Jun 28, 2019

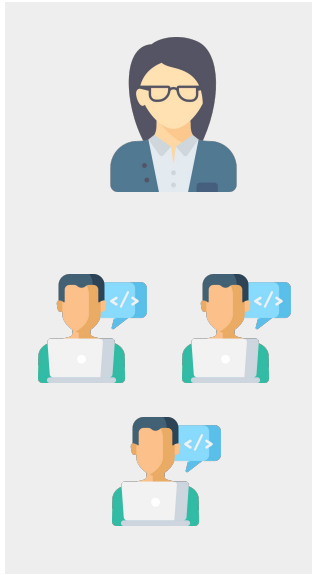
- FY2020 Q1 Customer Operations State of Security Report
- FY2020 Q1 Patient State of Security Report
- FY2020 Q1 Payer State of Security Report 2019-06
- FY2020 Q1 Pharmacy State of Security Report
- FY2020 Q1 Pharma State of Security Report - June 2019
- FY2020 Q1 Provider SoS - June 2019
- FY2020 Q1 - Specialty State of Security Report

API Security Recommendations - WIP

Created by Rachit Sood, last modified on Apr 16, 2019

DO's

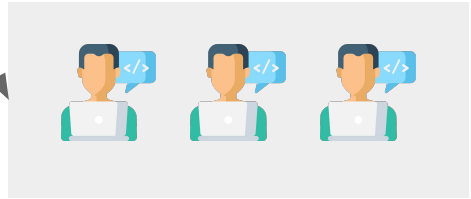
Level	Strategy	Definition	Where	When to use
No Auth	Tokens without secrets / API Keys	A static token (GUID) is sent with every request	Header	1) No PHI/No Risk if creds are compromised. 2) **Not recommended.**
Baseline	Basic Auth	Base64 encoded header with username+password is sent with every request	Authorization header	1) Low Risk if creds are compromised 2) API accepts data 3) B2B 4) API is internal only
Level 1	Username + Password	Authentication credentials sent in the payload with every request.	Body/ Payload sent with every request.	1) B2B 2) Externally facing API
Level 1.5	IP Whitelisting*	The IP of the calling application is checked on every request and compared against a preloaded set of IPs. Traffic from unknown APIs is rejected. **Must be used in addition to secret based authentication**	Application / Firewall/ Load Balancer / WAF	1) B2B 2) Client IPs are manageably low and do not change often/ static. 3) External API only 4) Use in addition to Basic / Username + Password
Level 2	Sessions	User has already established a session from a previous "recent" authentication. Expires.	Application	1) B2C 2) Browser Based Traffic 3) Single Page Apps / Client Heavy JS frameworks 4) External or Internal 5) Mobile Apps
Level 3	OAuth2 / OpenID Connect	Not a supported capability yet	Bearer Tokens (Dependent on the OAuth Flow in use)	1) B2C/ B2B4C 2) B2B 3) Mobile Apps
Level 4	Mutual Auth	Client is challenged to present a cert when negotiating TLS	WAF	1) B2B



Engineering

Product Leadership

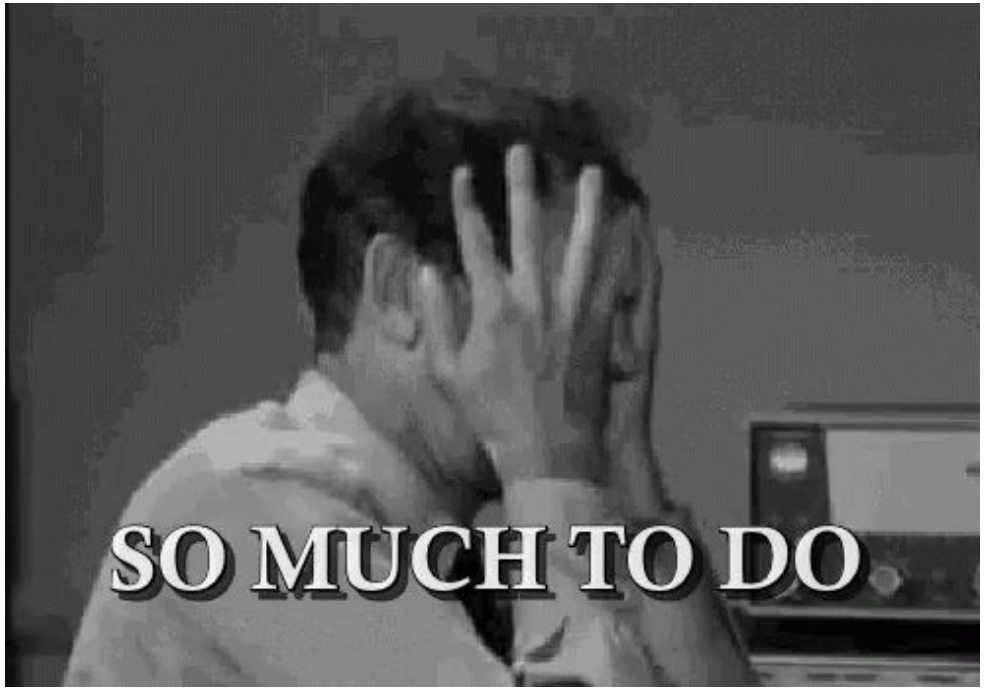
Security



Security Champions

Early Burdens

- Manual processes
- Heavy documentation burden
- Lack of insight into CI/CD scans
- Adhoc vulnerability management



Current State:

What It Looks Like Today

Our Champions

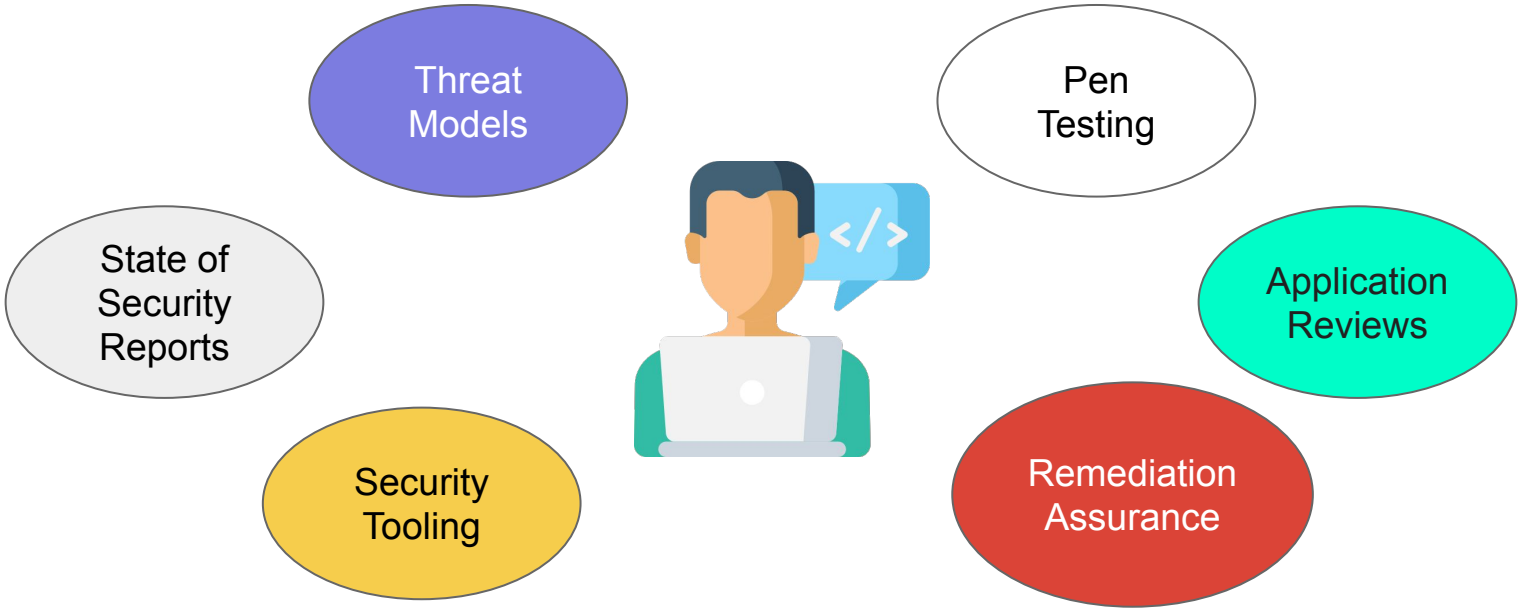
1 to 3 champions per dev team

Mostly developers

Not full time security resources

Their Responsibilities

Point of Contact for All Application Security Matters



App Sec's Role In All Of This

Build Relationships & Tools

Teach Security

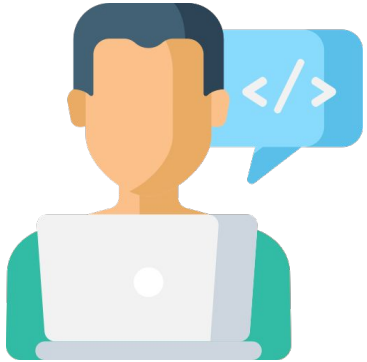
Mentor 1-1

Advocate for Devs

Advance Security Culture

Communicate

Drive Security Initiatives



WE GOTTA TALK

You now have an awesome

organic
information
radiator

Is it a lot of meetings? YES

Is it worth it? Totally

Can we work Async? YAASSSS!!

Daily

Slack Channels

Champions Helping Champions

Monthly

Security Working Group

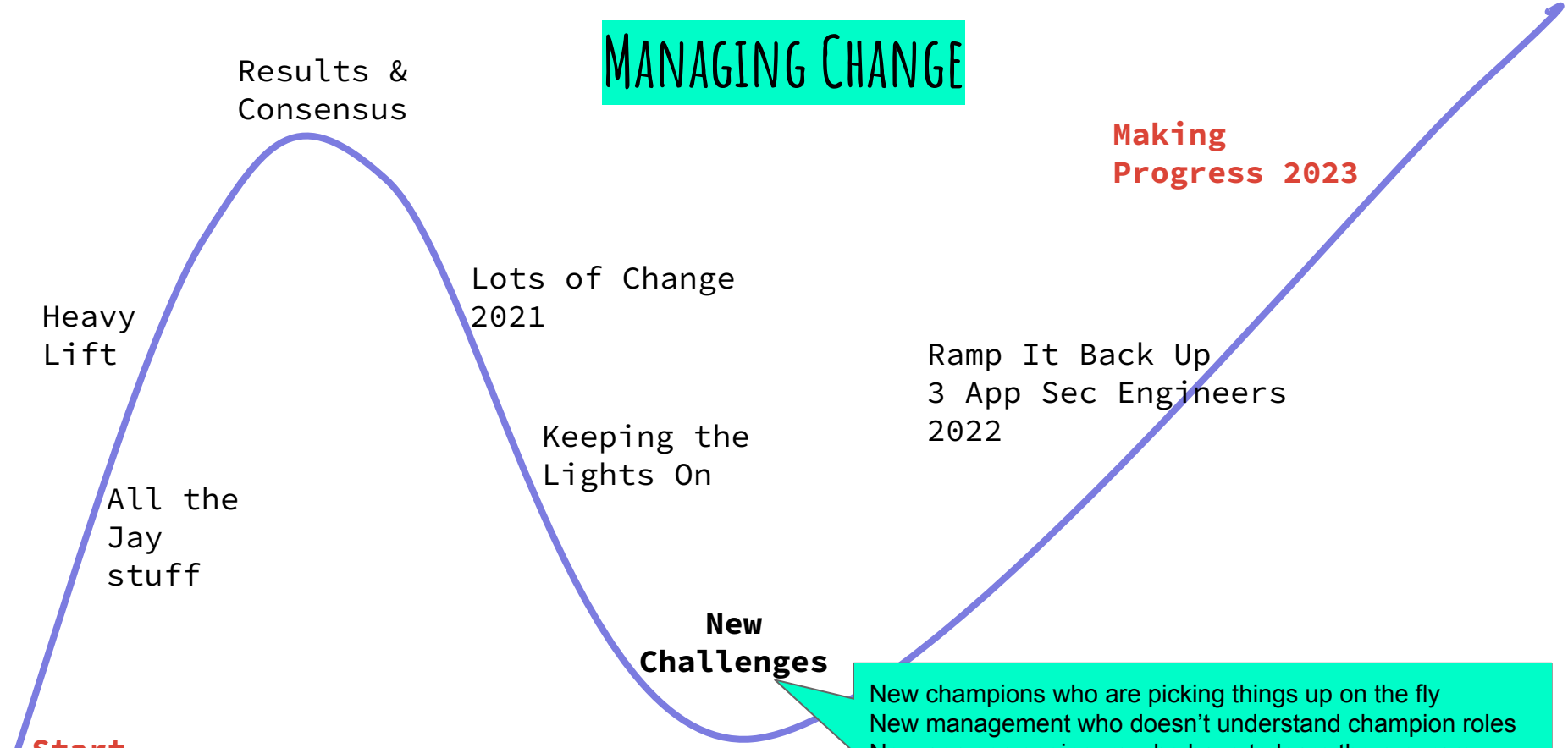
Security Community of Practice

Quarterly

Small Group Meetings

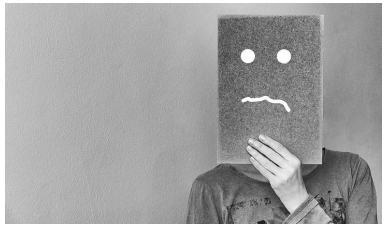
Day In, Day Out

Managing Change



New champions who are picking things up on the fly
New management who doesn't understand champion roles
New app sec engineers who have to learn the program
New parent company who has different tools and processes
New functionality
New tech and changing threat landscape

Burnout is real



Take a break

Rotate resources

Give feedback to management
(theirs and yours)

Add another champion to the team

Be flexible with tasks when possible

Jump in and do a little work for them

Recognize who is struggling and talk to them about it

Everyone Wins

Product

Better Risk Posture
Freedom to Innovate
Accelerated Growth

Security

Expanded Resources
Increased Productivity
Boots on the Ground

Engineering

Expanded Understanding
Increased Expertise
New Resources

Does any of this sound familiar?


Now what?

Where we want to go next...

Increased Participation in Community of Practice

Advanced Champion Designation

Security Champion Swag

More Risk Visibility

Threat Modeling Expertise

Intentional coaching

Greater Diversity

Branding

Outside Conferences & Training

Advanced Training Opportunities for Champions

Better Champion Recognition

Implement Champion Program Framework

WRAP-UP:

Value Delivery

TAKEAWAYS

An AppSec Program without Champions ≠ Scalable

You can start a Champions Program - We did!

You have to Keep Learning and sharing knowledge

Help is out there for just about everything

Product Security Is Here to Stay!

Our Favorite Resources

1. Application Security Podcast - Chris Romeo
   https://www.securityjourney.com/resources/application-security-podcast

2. We Hack Purple - Tanya Janca
   https://wehackpurple.com/

3. Building Security In Maturity Model (BSIMM)
   https://www.bsimm.com/

4. Open Web Application Security Project
   https://owasp.org/

   - Application Security Verification Standard
   - Web Security Testing Guide
   - Application Security Guide for CISO's

Q&A