

# Security Champions

Enabling Product Teams to Move Securely

Steven Carlson - 2023

# Overview

## The plan

- **Goal** - What does good look like
- **Program** - Operationalization
- **Roll-out** - Maturing the program
- **Lessons Learned** - Please don't make my mistakes

# Terms

## Common Language

- AppSec is about securing the application.
- DevSec is about securing the developer and their actions.
- DevSecOps is about securing the application build chain.
- Product Security is about the end-to-end security of their organization's software products.

# Product Security

# We, the Security Team

## Recognize That Engineering Teams

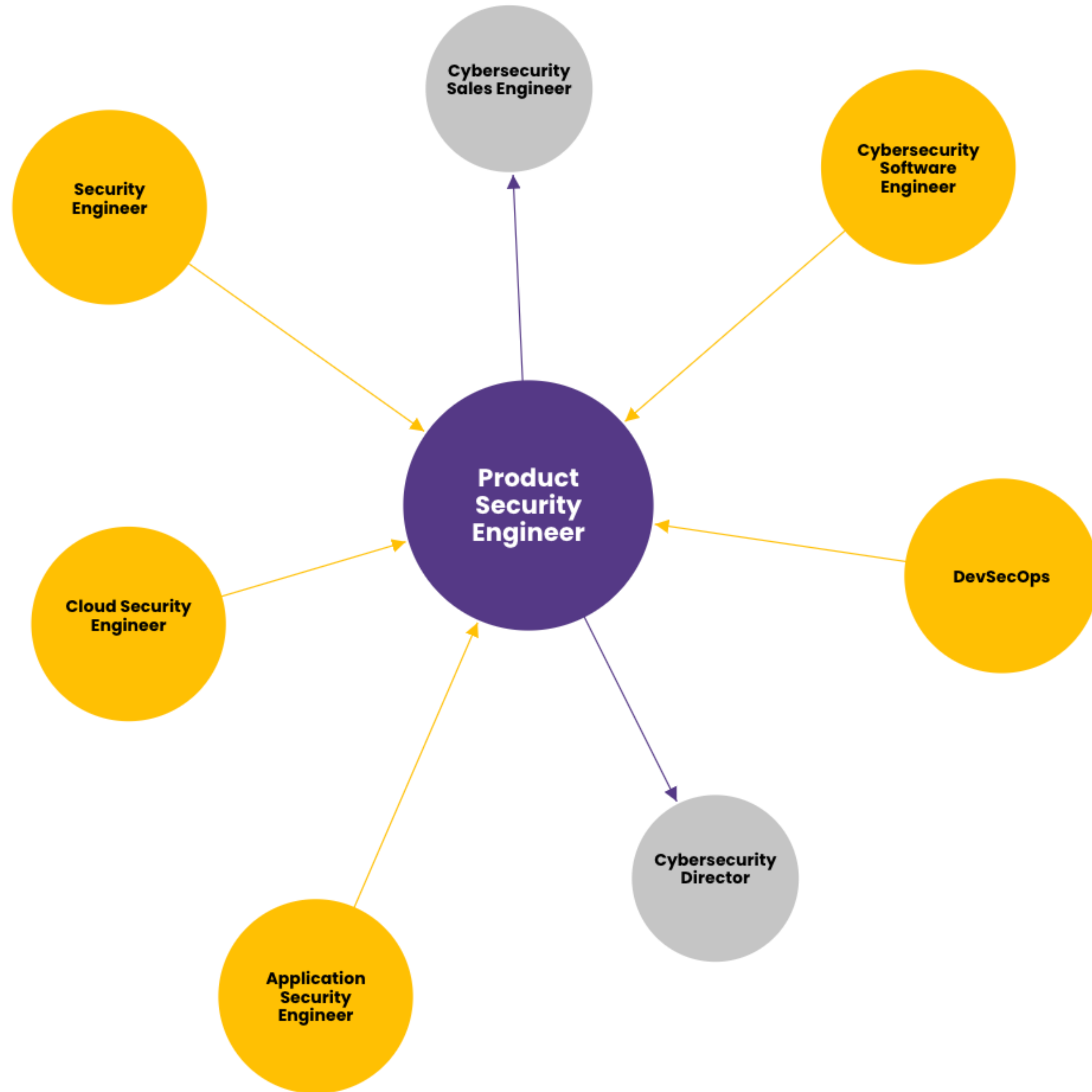
- Want to do the right thing
- Are closer to the business context and will make trade-off decisions between security and other tasks
- Want information and advice so those trade-off decisions are more informed

## Pledge to

- Lower the cost/effort side of any investment in developer security tools or practices
- Assist 2x as much with preventative initiatives as we beg for your assistance reacting to security incidents

## Understand that

- We are no longer gate keepers, but rather tool-smiths and advisors



# Goal

# What is a Security Champion Program?

## Ideal state

- Create a clear picture of a product's risk profile for both product and security leadership.
- Champion(s) will share ownership of the product's overall security score card along with the Information Security team.
- Become a threat Intel feed for the larger Information Security Department.
- Recommend policy and standard modification to meet their product teams needs.
- Actively enhance a product's overall security footprint while working with product manager(s).





**Not just knighting someone, a shared partnership**

# Program

# How should we structure the program?

## Things to consider

- Identify teams and stakeholders
- Define champion's role
- Nominate champions
- Establish a communication channel
- Build a solid knowledge base
- Maintain interest
- Clear security goals to work towards
- Schedule training and interviews with information security department staff
- Work with leadership to allow time for security work
- Get political support
- Build a Career path



# 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

# OWASP

**<https://github.com/c0rdis/security-champions-playbook/tree/master/Security%20Playbook>**

# Roll-out

# What are the activities we should focus on?

## Short to long term

- Review existing partnerships within the organization and invest in the people.
- Pilot the program with one product team and share on its success.
- Work with information security leadership to get buy-in from executive leadership.

# What should the champion lead focus on?

## Optimizations or short term wins

- Start from most left and work right: (Owner - Threat - Automation - Runtime).
- Lead conversation(s) focusing on existing and future: (Current -> New).
- Leverage existing partnerships to bring talent the surface: (Introverts).



# Growth Strategy

- **Listen, Partner, and ask Questions**

- Regular meetings with engineering leadership
- Secure code is a form of “code quality”
- Seamless experience/remove friction

- **Training (Targeted Education)**

- Web App pen testing training
- Monthly / Hack Club meetings
- Secure Coding training

- **Secret Sauce**

- Matrixed working group aka product teams
- Word-Marketing: Security Assessment/ Evaluations Points vs. Security Toll Gates
- Training dollars – sourced from my security budget

# Lessons Learned

# Executive Leadership

## Top down must go with button up

- Place your leaders into bucket of trust before kicking off the program (partners, opportunities, and red herring).
- Focus on the opportunities bucket and practice idea(s) with partners bucket.
- Even if you have CISO buy-in, middle management needs to be treated with white gloves.
- Always follow up with pending questions, even if you don't have a direct answer.

# Start with Small Templates

## **Allow champions to share in the story**

- Don't try to eat the whale in one bite. Bring the whole family and take a lot of small bites.
- If you solve a problem for one team, allow that team to present the topic to the next team.
- Share the success with security leadership and provide a small token of appreciation to each person.

# Knowledge Base

## Sharing is caring

- Encourage champions to contribute to knowledge base.
- Record the audio and transcript of each session.
- Keep attendance and share with compliance / legal.
- Create an on-boarding presentation before hosting a kick-off.

# Manifesto

# Manifesto

- Build security as more than bolt it on.
- Rely on empowered product teams more than security specialists.
- Implement features securely more than security features.
- Rely on continuously learning more than end-of-phase gates.
- Adopt a few key practices deeply and universally more than a comprehensive set poorly and sporadically.
- Build on culture change more than policy enforcement.

# Questions?

**I see you**