



# **Using Security Champions to Build a DevSecOps Culture Within Your Organization**

**Brendan Sheairs, Managing Consultant, Synopsys  
March 14, 2019**

# Introduction—Brendan Sheairs



Managing consultant at Synopsys

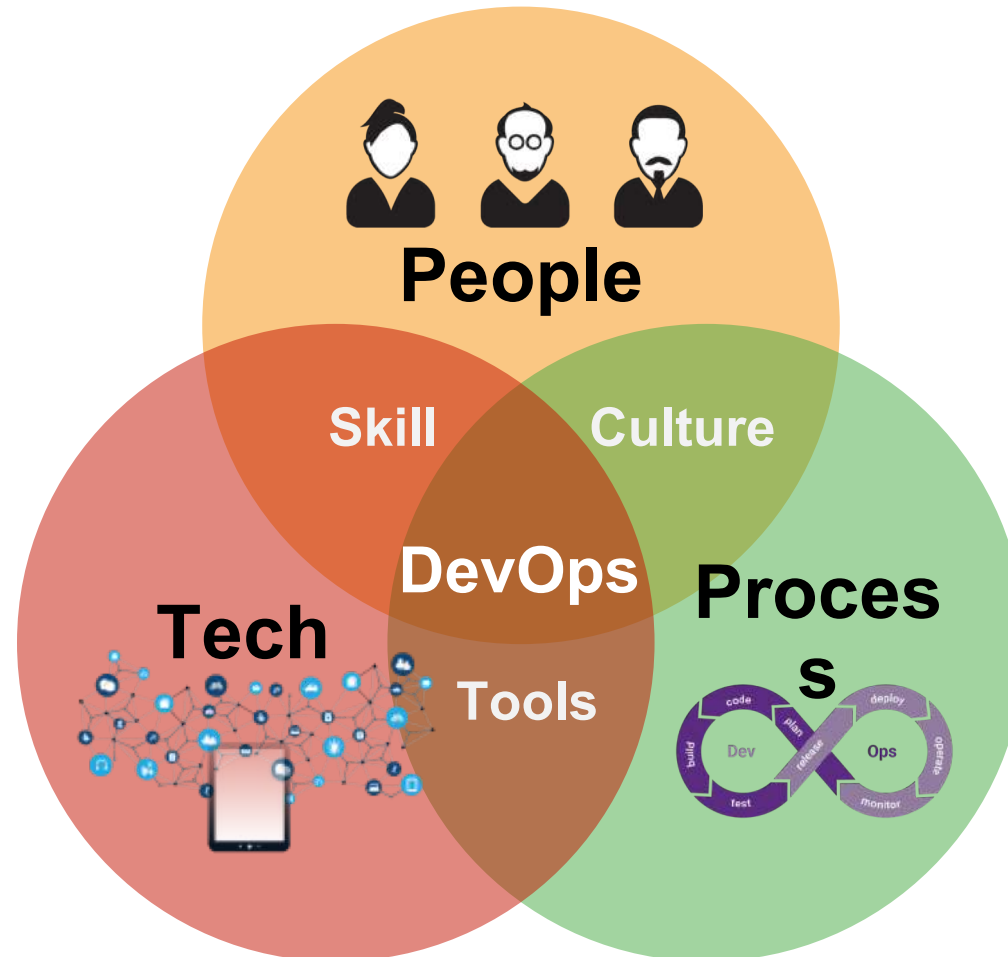
Have been with Synopsys  
(*previously Cigital*) since 2011

Over the past three years, have worked closely with several Fortune 50 companies to design, implement, and manage Security Champion programs

Responsible for delivery oversight and support for Mid-Atlantic region

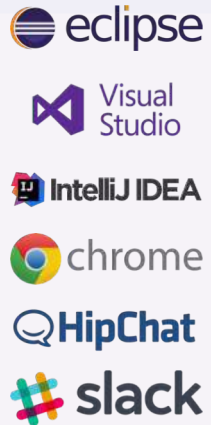
**SYNOPSYS**<sup>®</sup>  
*Silicon to Software*<sup>™</sup>

# DevSecOps overview





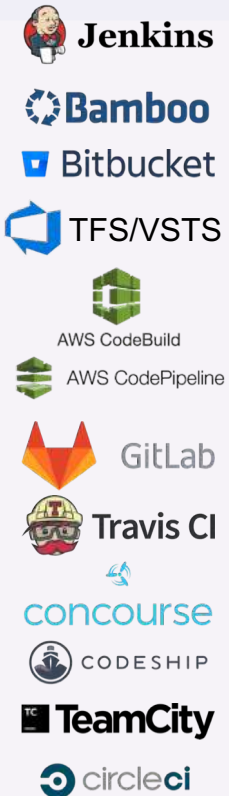
DEV / IDE



SCM



Build / CI



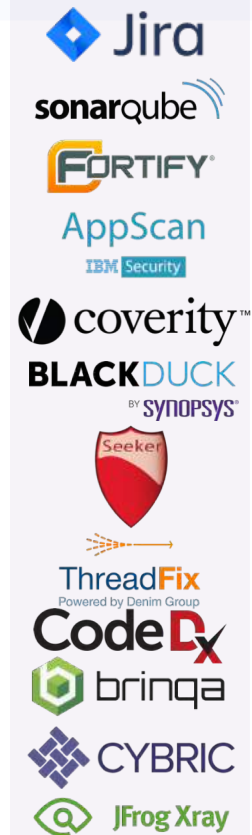
Container / binary repositories



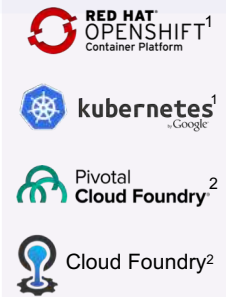
Package management



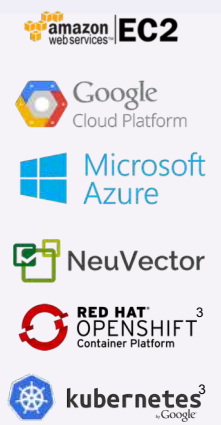
QA



Orchestration



Production



<sup>1</sup> Automatic Image scanning during orchestration  
<sup>2</sup> Automatic droplet scanning during of push  
<sup>3</sup> Deployable on these platforms

# Challenges of building security into DevSecOps

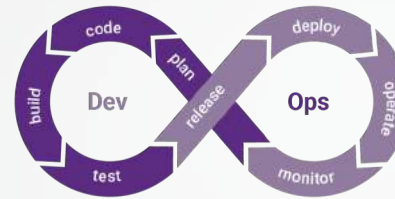


## People

**Developers emphasize functionality over security.**

Security experts are often seen as an impediment to business goals.

Organizations have limited software security resources.



## Process

**SDLC methodologies play a huge part in defining the CI/CD workflow of application security tools.**

No standardized defect tracking for security defects.

Applications are NOT classified into tiers to prioritize assessment scope.

No standardized metrics dashboard for quality and security defects.



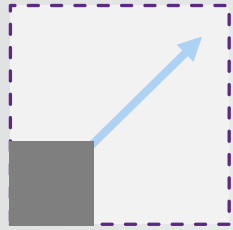
## Technology

Tools aren't a catch-all solution; they can't interpret results, find architecture and design flaws, or certify that the code is free of defects.

**Tools suffer from false positives and false negatives.**

Organizations use different languages, which means different build tools.

# Common challenges of software security groups



## Scale

Difficult to find AppSec professionals

Application portfolio coverage gaps

Large technical security debt

**High consultation load on SSG**



## Agile

**Security is struggling to keep pace**

Issues with security tool adoption



## Developer relations

Reactive, not collaborative

**Security is engaged late in the release cycle**

Reactive engagement causes product release delays



**How can we address these challenges?**

# Security Champions





# Security Champions (satellite) —as defined by the BSIMM

A **group** of interested and engaged **developers** who have a natural affinity for **software security** and are **organized** and **leveraged** by a software security group.

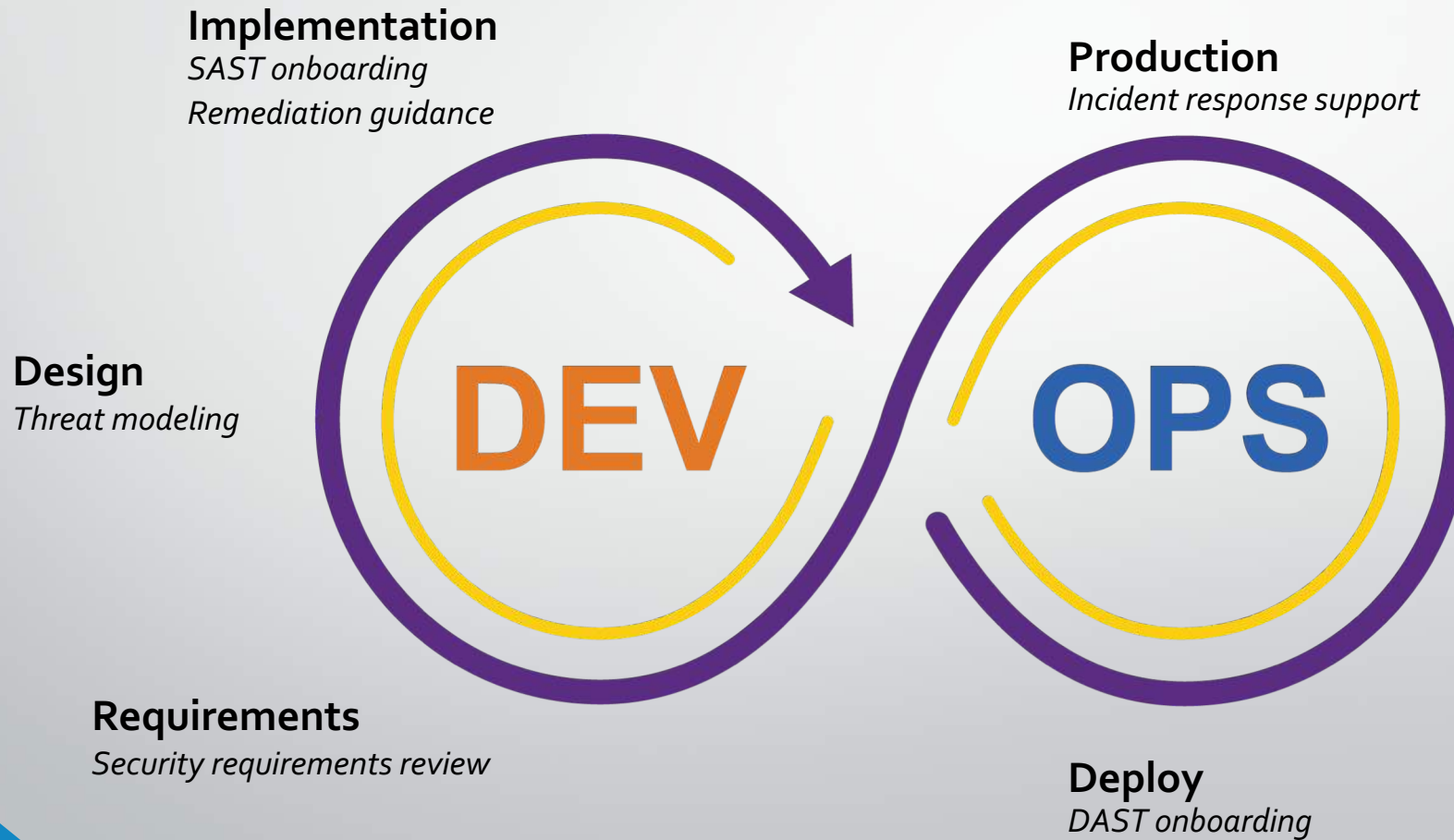


# Benefits of deploying Security Champions

- Scale
- Reducing friction
- Hands-on security support
- Increased vulnerability remediation



# What does a Security Champion do?





**What are the qualities of a strong Champions program?**

# Who are good Security Champions?



- Full-time employees with experience in the software development organization
- 3–5 years of software development experience
- Strong communication and organizational skills
- Demonstration of application security aptitude

# Qualities of a strong Champions program



## Leadership

- Defined roles and responsibilities
- Metrics to track program impact

## Growth

- Progression and structure to focus skill development
- Training to provide software security foundation

## Community

- Support for Champions and continuous education

# Security Champion progression

## Level 1—**Foundation**

Focus on gaining experience and remediation guidance



## Level 2—**Skilled**

Leverage experience for more complicated activities  
Build security into CI/CD pipelines and SDLC

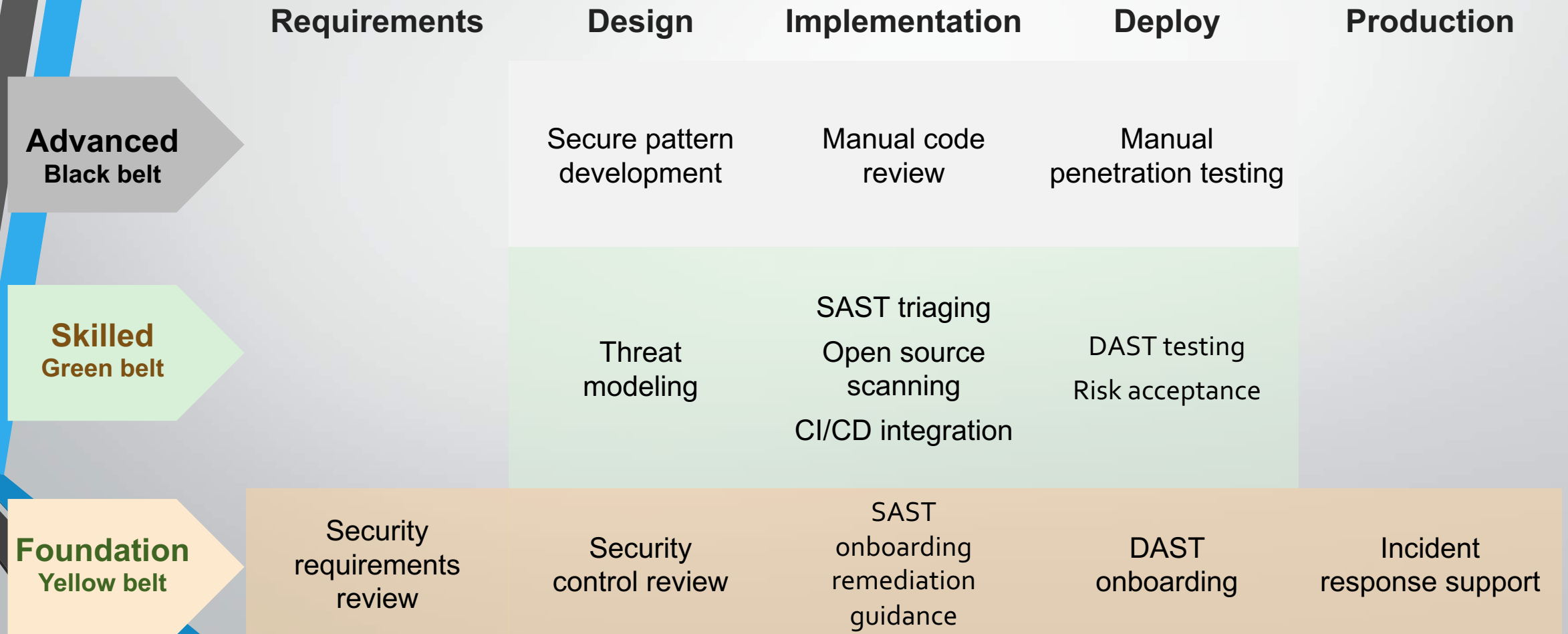


## Level 3—**Advanced**

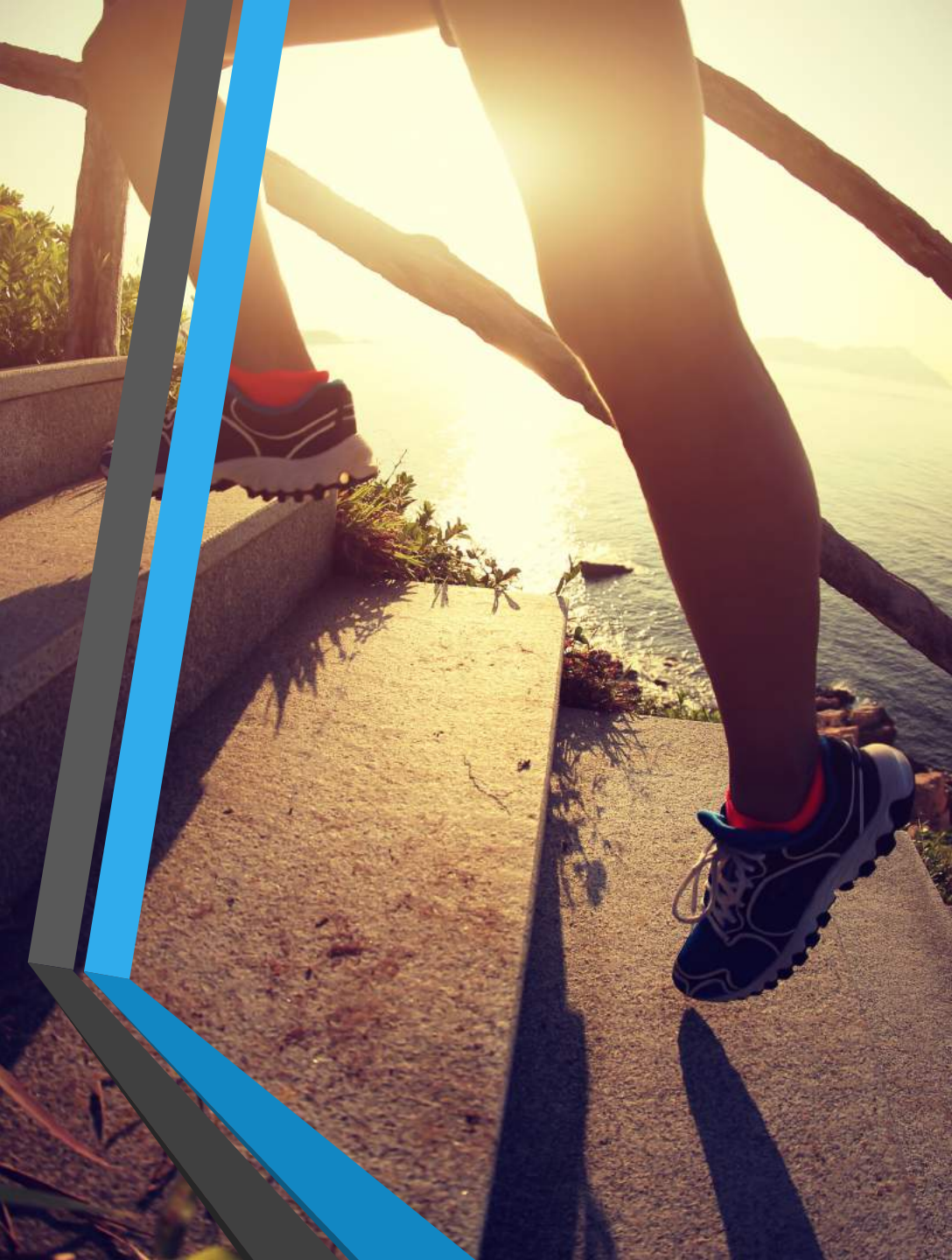
Shared ownership of more advanced security activities



# Security Champion progression + activities







# Training

Provide training based on the activities defined in your program

Provide a mixture of eLearning and instructor-led training

Provide hands-on exercises

Scale training based on Champion level

# Security Champion program roles overview

Security Champion Program Lead

Security Champion Coaches

Security Champions

# Community


Community meetings

Quarterly metric reporting

Community forum

Community portal





**How do I know if my Champions  
are having the right impact?**

# Security Champion metrics

## **Maturity**

Measures adoption, coverage, engagement of Champions, etc.

## **Impact**

Measures effectiveness





**How do I get started?**

# Defining your Security Champions program

*Two major parameters to consider:*

## **Breadth versus depth of duties**

Should Security Champions remain primarily as developers with a focus on security?

*Or should they focus on performing activities as embedded security people?*

## **Time commitment**

What percentage of their job will be spent on Champion-related activities?



# Deploying your Security Champions program



- 1. Understand** process gaps
- 2. Comprehend** dev challenges
- 3. Define** goals
- 4. Establish** responsibilities
- 5. Achieve** program buy-in
- 6. Pilot** the program
- 7. Grow** and scale the program



# Thank You

**Brendan Sheairs**  
Managing Consultant,  
Software Integrity Group  
*bsheairs@synopsys.com*

<http://www.synopsys.com/software>