

5 Steps to

Build a World-Class Security Champion Program



by  apiiro

Welcome!

The concept of “Shift Left” security has been permeating the AppSec community for quite some time. The high-level concept is sound: the earlier you identify vulnerabilities and other security weaknesses, the faster you can remediate the issues, leading to less re-work, lower costs, and increased speed.

But there is a concept that is a core component of the Shift Left ideal that is often neglected: Developer Empowerment. The most effective AppSec program is one that gives its developers the training and context they need to make smarter security decisions from the start.

One of the best ways to do this is with a robust Security Champions program. Imagine having security experts embedded in your Engineering teams, each of whom is available to other developers as a reviewer, coach, and mentor. They are given exactly the right information to understand what each member of their team is doing that may affect the security of your applications and infrastructure so they can step in at exactly the right time. This is what a strong Security Champion program provides you.

Until now, identifying and enabling Security Champions has been too difficult – and establishing a program has been just out of reach in a growing list of priorities. Apiiro can help. We can identify your potential Security Champions without manual surveys and questionnaires; we identify your security experts by looking directly at the code. We then help you put your Security Champions in a position to succeed.

Security and Development teams have too often been at odds, with Security seen as a blocker to progress. With the new level of communication and collaboration that is now possible between teams, you can put that conflict in the rear-view mirror and work together to accelerate product delivery and securely enable digital transformation.

A Security Champions program can help you whether you have a mature and measurable Application Security program or are just getting started. Read on to learn about the concrete steps you can take to build security into your Development process – from the start.

Idan Plotnik,
Co-Founder & CEO



Table of Contents

5 Steps to Build a World-Class Security Champion Program

Introduction	04	Overview
The 5 Steps	05	<ul style="list-style-type: none">1. Define Success2. Identify Security Champions3. Provide continuous training4. Give them visibility and focus5. Empower them
Take aways	13	How Apiiro Can Help
About Apiiro	14	Apiiro solutions

04

Overview

“Security Champion” is a bit of a nebulous term. To some, it can be applied to any number of people in various roles. To others, it is a very concrete position with specific responsibilities. Without an industry-standard definition, it is up to each organization to define and build a Security Champions program in a way that best aligns with its goals and culture. That said, there are some specific guidelines that organizations can follow that will help them ensure the success of their program.

Organizations that follow this process will embed security deeply into their operations and transform their security programs – whether they are already mature or just getting started. Security vulnerabilities and risks will be identified earlier in the process and on-going learning will improve security from the design stage to coding to production infrastructure. Feedback loops will ensure continuous improvement and lead to improved security, minimized rework, and reduced costs – all while delivering faster than ever.

Read on for details on each step to building a World-Class Security Champions Program.

Five Steps to Build a World-Class Security Champions Program



05

1.1 Define Success

The first step in the success of just about any program is to define your criteria for success. What are you trying to accomplish? This may vary widely depending on the security maturity of your organization. If you are small, growing fast, and have an immature security function, your needs are far different than those of a mature organization that's looking for a new way to inject security-related thinking into their already-established teams.

Here are some questions you may want to consider:

- ✓ What is driving the need for security in my organization? Is it risk management, regulatory requirements, specific customer demands, or something else?
- ✓ How much of a priority is security to my organization? Do I have the mandate to make significant changes?
- ✓ How is security perceived culturally in my organization? Are people enthusiastic about security? Is it considered a burden that gets in the way of getting "real work" done or does everyone understand its importance?
- ✓ How knowledgeable are my developers and other contributors when it comes to security?
- ✓ How mature is my security program and how far do I have to go until we reach our goals?
- ✓ How will executives and other senior leaders perceive a Security Champions program and what will key stakeholders expect from the program?
- ✓ How will I measure results?

06

1.2 Define Success

Measuring results is essential and should be done before putting your program in place. First, consider the overall goals of your Application Security program. These metrics should be risk-based and avoid the traditional “vanity metrics” of legacy AppSec programs, such as the number of vulnerabilities remediated in a month or mean time to resolution. Instead, metrics need to be risk-based and factor in the business impact of a vulnerability or weakness. A successful Security Champions program should have a clear and measurable impact on your overall Application Security program metrics.

Tracking the impact of individual Security Champions is also important, in order to discover where additional coaching may be needed. Some key items to measure include:

Some key items to measure include:



Team security KPIs, such as security-related defect rates



Improvements in individual developer security expertise and knowledge



The number of instances a Security Champion has been involved in helping teammates with Security-related issues

07

2.1 Identify Security Champions

Once key goals are defined, choosing the right people to be Security Champions is critical to the success of the program. This must be done in a way that combines technical knowledge with enthusiasm and the willingness to become a security evangelist inside the organization.

On a technical level, one often-overlooked way to identify potential Security Champions is to look at the code! See which developers are working with PII, modifying sensitive APIs, using authentication and authorization controls, etc. You can also look at past commits to see which developers are prone to writing and committing code with security weaknesses and which are not.

On a personal level, being a Security Champion is a role that requires buy-in! A person with extensive security knowledge will never succeed as a Champion without the desire to share their knowledge with others on the team.

Contributors 6 / 2650

Ben Jameson ★ Security Champion
1234 Commits · 885 Pull Requests · 4 Repositories · 14 Technologies

Anastasia Shore
841 Commits · 632 Pull Requests · 5 Repositories · 18 Technologies

Jennifer Green
234 Commits · 185 Pull Requests · 4 Repositories · 14 Technologies

Search filters

Time Frame
Apr 1, 2021 - Jun 30, 2021 +

Contributions

- ☐ APIs
- ☒ Authentication
- ☒ Authorization
- ☒ PII
- ☒ Security

See more...

Identify potential Security Champions
by looking at their code!

07

2.2 Identify Security Champions

While official “Security Champions” may be developers in many organizations, it’s also essential to look beyond engineers! Any number of people and roles can identify security risks and become experts in risk mitigation, including:

Full-Stack Engineers

QA Testers

Application Architects

Designers

DevOps Engineers

Product Managers

Program & Project Managers

Documentation Specialists

Customer Success Managers



You will need to decide how extensive a program you want to build and what is the right fit for your organization. You may also start small and focus on only one or two roles before expanding to the larger team.

08

3.1

Provide continuous training

Security is an ever-evolving field. New attack techniques and vulnerabilities are discovered regularly and your Security Champions need to be kept up-to-date on the latest security trends. There are three primary aspects to ongoing learning:

1. Team Training

2. Individual Training

3. Information Sharing



Team Training

1. Team Training

Establish a baseline for security knowledge and rally around a set of approaches and philosophies. This is often implemented in required security training that everyone takes (and needs to receive a passing score). It could be based on concepts like “Security by Design”, “Build Security In”, or another philosophy or training program. All team members should go through the same basic training program so you can standardize on a common language and way to approach security problems. This training can be performed in person, remotely, or even using online training systems.

High-level security training is important but it CANNOT be restricted to broad-brush computer-led modules. While having a baseline is important, it’s not nearly enough to ensure your Security Champions are true experts in the field.

09

3.2

Provide continuous training

2. Individual Training

The next level of training consists of levels. This is often implemented in a martial arts-style belt system, from “White Belt” to “Black Belt”. These types of programs add significant value! Not only do they give individuals something to strive for, but they give leaders the opportunity to publicly congratulate individuals as they work their way up the expertise hierarchy. Going beyond internal training is also critical for many members of the team, so many organizations provide training time and expense reimbursement for industry-standard certifications such as the CISSP and others. Unfortunately, belt-style systems and certifications are not yet enough to build effective Security Champions.

The final, and optimal level of training is completely personalized and contextual. Imagine a full-time security coach looking over the shoulders of your developers (and other Security Champions!).

New Workflow ·

Workflow Name

Given

Commit


In product

When

Has Label

PII added

Then

 Slack Message

on

#channelName

and mention

Developer

to

Take Cloud Infrastructure Configuration Security Training Module

Developer training should be automated & personalized

They could provide the right security tips and insights to each individual at exactly the right time. While this is not a scalable solution, it is absolutely something we can automate with a deep enough understanding of your applications and code!

Consider a developer who writes code in a new language for the first time? Or works with a new authentication or authorization framework? The right time to provide security training for that developer is at the time they are writing the code. Waiting until vulnerabilities are introduced and going back to provide training is inefficient, costly, and slows down delivery.

10

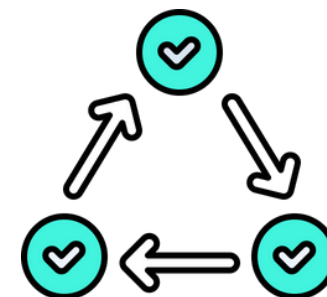
3.3

Provide continuous training

3. Information Sharing

Information sharing is often an overlooked component of a Security Champion program. At the most basic level, provide regular team meetings for Security Champions across your organization to share their learnings, successes, and failures. Use mailing lists, chat groups, newsletters, wikis, and other forums to give the extended team a sense of identity and belonging.

There are people in your organization who are experts in specific technologies and frameworks - make it easy to share that knowledge! If a developer starts writing a certain type of security control in a particular language, alert them that one of their peers has experience in that exact area.



11

4. Give your Security Champions visibility and focus

In order to be effective, Security Champions need to have visibility into risk and know where to focus their attention. Security knowledge used haphazardly is inefficient and a waste of time and expertise. Ensure that your Security Champions have deep visibility into the risks of their applications. This doesn't mean to only provide them with scan results from SAST, SCA, and other tools, but to give them insights to understand the true risk of their applications on a business level. This includes understanding which of their applications:

----- **Store and/or process PII**

----- **Are Internet-facing**

----- **Are protected by an API gateway with authentication and authorization controls**

----- **Are subject to specific regulations**

----- **And more!**

In addition to giving your Security Champions visibility into risk, you need to help them prioritize those risks by giving them access to the relevant context. Looking only at code is not enough because risk is multidimensional. It requires an understanding of

everything from the developers working on the application to the production infrastructure settings. Attackers don't look for security vulnerabilities and weaknesses in isolation and neither should your Security Champions.



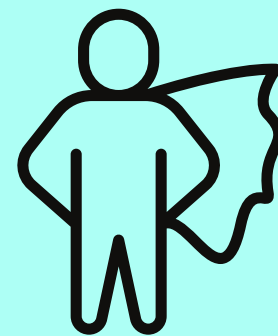
12

5. Empower your Security Champions

Finally, Security Champions in your organization have to have the authority to make an impact! Many hours of training and access to numerous security tools and information is worthless if your organization is not structured in a way to make use of all that knowledge.

Security and risk management are critical to business success in nearly all organizations, but there are competing interests and priorities as well. There are features that need to be developed and delivery timelines that must be met.

An effective Security Champions program must have a mechanism to ensure that security concerns are heard and addressed. In some organizations, Security Champions may need the authority to halt a release, regardless of seniority. In others, the Security Champions can be given a direct line of communication to senior leaders who have go/no-go decision authority.



Make sure you publicize success so that every member of the team feels empowered to identify and address security risks. Recognition is a powerful tool to motivate not only the existing Security Champions but recruit new members.

13

How Apiiro can help

Apiiro is re-inventing the Secure Development lifecycle for agile and cloud-native development. The Apiiro Code Risk Platform™ is uniquely suited to help organizations build a Security Champions program because it has an in-depth understanding of both code and applications at a technical level, but also in its understanding of developers and other contributors.

If you're interested in learning how Apiiro can help you build a Security Champion program, schedule a demo today!

Schedule a demo



Apiiro helps you:

Define Success by providing you with risk-based visibility into your applications and infrastructure. By understanding the business impact of changes across the SDLC, Apiiro helps you create and measure a new level of metrics that are tied directly to your business risk. With a risk-based and measurable Application Security program, you can build a more effective Security Champions program.

Identify Security Champions by analyzing all of your applications, repositories, and individual commits to uncover individuals with security expertise.

Provide continuous training by identifying areas for improvement and triggering workflows that recommend appropriate areas for security training.

Give them visibility and focus by providing a unified, risk-based work plan and alerting Security Champions to areas that require their attention - directly in a commit message, pull request, or messaging system (including Slack and Microsoft Teams)

Empower them by providing business-level, risk-based reporting that continuously demonstrates the value of your Application Security and Security Champions programs.

About Apiiro

Apiiro helps you build a risk-based & measurable AppSec program. Our Application Risk Management platform provides complete risk visibility & control, from design to code to cloud. Our multidimensional approach to application security will help accelerate application delivery while reducing costs and risk.

Apiiro is re-inventing the secure development lifecycle for agile and cloud-native development, with 5 solutions:

Application Inventory & Asset Discovery Define Success with risk-based metrics that help you measure your AppSec program at both business & technical levels & Gain Risk-Based Visibility

Risk Assessment & Change Management Automate Code Governance with detailed workflows and a flexible Code Governance Engine

Security & Compliance Assurance Remediate Risks that Matter, with a risk-based Remediation Work Plan

Git & CI/CD Security and Integrity Shift Left & Extend Right with Security Champion identification and the context to trigger context-sensitive developer training

SSDLC Processes & Tools Orchestration Approach the SSDLC holistically with a risk dashboard that covers all SSDLC processes



Apiiro solutions

[Learn More](#) →

Application Inventory & Asset Discovery

Gain Risk-Based Visibility, with a Real-Time Inventory

112 Developers in 3 risky applications
Contributed authorization & authentication changes

View Profiles

13

PII Fields
Written to logs

21

Exposed
Secrets

5

Vulnerable
Dependencies

Risk Score

7.8

High

PCI data exposed by an API
Missing input validation

5/214 findings relate to internet-facing APIs

3/46 findings relate to sensitive dependencies

Repository Behavioral Profile

4 Abnormal Commits

Abnormal Commit e32298e

Committed authorization changes on non-Working Hours [View Timeline](#)

JonathanR FrontEnd developer usually commits UI changes [View Profile](#)

Create a new governance rule

PII Exposure

1 Define Scope

For All Applications

2

3 Select Risk Factors

API that is Internet-Facing is Exposing PII and Missing authorization

4 Trigger Actions (optional)

☐ Comment on the Pull Request

Manage Risk

Accept or reject risk or trigger remediation actions

Attack Surface Elements	% of Elements	Source	Security Process	Risk
Internet-facing APIs With Vulnerabilities 12 elements	6%		Vulnerability Remediation	
Cloud Database Misconfiguration 8 elements	3%		Cloud Security Review	
Dependencies with Vulnerabilities 6 elements	9%		Security Code Review	
Exposed Secrets in Source Code 24 elements	12%		Security Code Review	
PII written to logs 13 elements	2%		Compliance Review	
Upcoming Risky User Stories 3 elements	2%			

Top Risks by SSDLC Process

Security Review

178 Exposed secrets in source code

86 PII Exposed by an API

74 Payments Data written to logs

Select an SSDLC process

Security Review

Pen Test

Cloud Review

Compliance Review

6

14 Products

▲ 3%

Start Remediating Exposed Secrets in Source Code

Create a workflow