Introducing Security Champions to the DevSecOps Life Cycle

By Brendan Sheairs

Table of Contents

A 2015 Gartner report estimated that 25% of Global 2000 organizations would be using DevOps and Agile development practices as part of their mainstream strategies by the close of 2016. Our experience with Black Duck customers confirms this prediction has come true.

In Agile development, passes through the software development life cycle (SDLC) occur more often than in traditional development models. Some development teams complete an SDLC over the course of 2 weeks, while others complete one daily.

A traditional software security group (SSG) isn't equipped to apply security activities to Agile development environments effectively. Applying security to agile processes requires the injection of security-related people, processes, and testing activities at a sprint tempo. This tempo leaves little time for security teams and resources to review the software, deliver information on security and quality defects, and retest without disrupting the workflow. Even if SSGs dedicate staff to each project (which is usually out of the question), there still isn't enough local knowledge of each application to get everything done well.

So how can we inject security into Agile development?

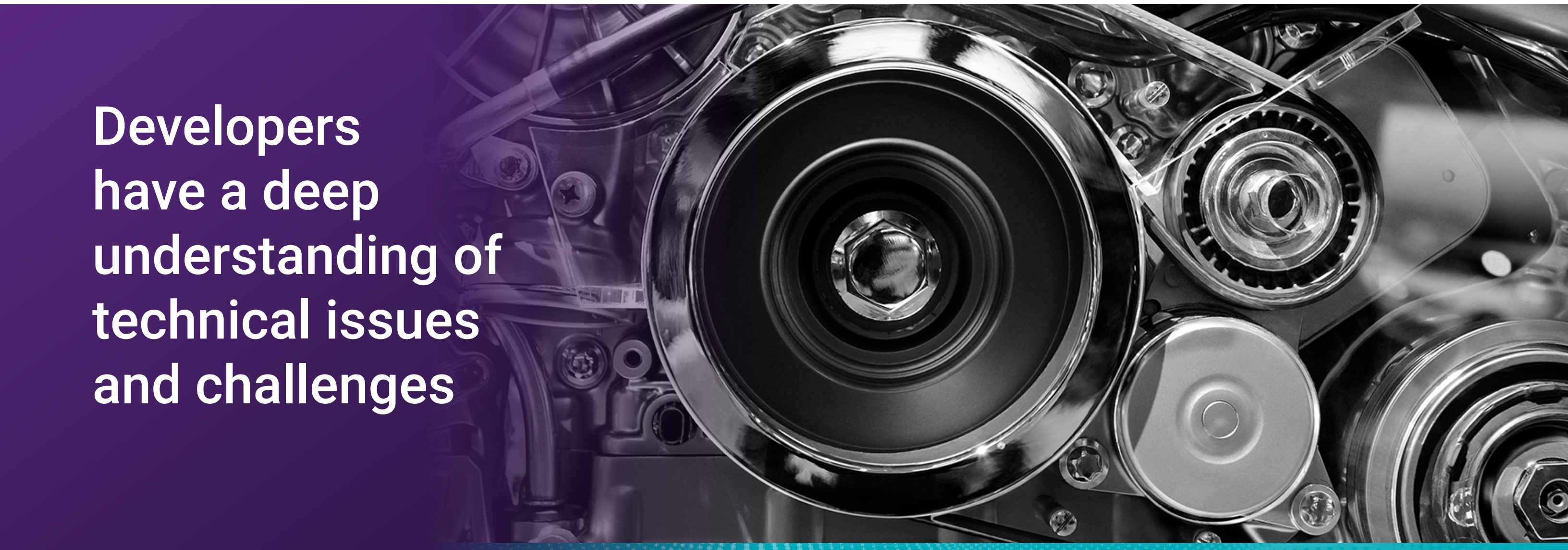
Enlist developers.

Developers are familiar with an organization's software. They are familiar with the organization's development groups. And they have a deeper understanding of the technical issues and challenges that the organization faces. Recruit these developers as Security Champions. Train them in defensive programming and how to identify security defects. Additionally, empower them with responsibility for the security of the applications they work on.

What are Security Champions?

Security Champions are developers who have a direct impact on the resiliency and security of their firm's software. They are enthusiastic volunteers willing to participate in advanced software security training to perform an important role. They are also a part of a greater community of Champions exchanging ideas and techniques.

Since Security Champions come from within the development organization, they have the right relationships to better assist developers, testers, and architects in accomplishing their goals. Security Champions can usually communicate more effectively with software teams than the centralized SSG can.



Developers have a deep understanding of technical issues and challenges

How do you design a successful Security Champions program?

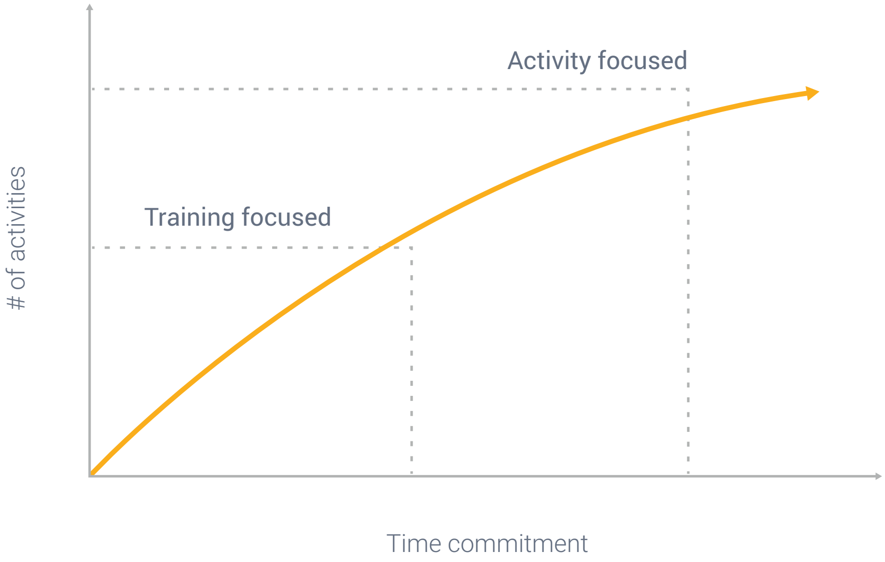
Consider these two important parameters when designing a Security Champions program:

1. **Breadth versus depth of duties.** Should Security Champions serve primarily as developers with a focus on security? Should they concentrate on performing all the secure development activities on behalf of their teams? Or should they be responsible for security activities across multiple teams as embedded security personnel?

2. **Time commitment.** It's important to consider how much time Security Champions will need in order to perform the duties outlined above. Should they be part-time or full-time?

These parameters are major factors in the design of your organization's Security Champions program. You might have Champions who work primarily as developers but also play a larger role ensuring their applications are secure. Or your Champions might spend all their time performing security reviews, providing remediation assistance, and training developers across a portfolio of applications.

Among our customers, we have observed three primary types of programs: training-focused programs, activity-focused programs, and hybrid programs.



To determine the best approach for your organization, start by clearly defining your Security Champions program goals. Do you need to scale a comprehensive set of security activities across the organization to keep pace with agile teams using dedicated staff? Or would you rather focus on training developers to be more security minded when they write code?

Training-focused programs

In a training-focused program, developers undergo advanced training through eLearning and/or instructor-led courses. Once the initial training is complete, they resume their development responsibilities, backed by a Security Champions

community to whom they can reach out for support. After initial training, Champions should also attend periodic technical talks and events to stay current on industry trends and new risks.

Merits of the training-focused approach:

- Requires minimal time commitment after initial training
- Contributes a resource to development teams who can drive the adoption of security requirements, policies, and tools
- Imposes a low cost on the organization
- Provides a source of feedback to help improve the SSG's impact

Activity-focused programs

At the other end of the spectrum are activity-focused programs. This approach builds on the same training but extends its reach to encompass all secure development activities for a collection of teams. In this approach, Champions are assigned a portfolio of applications—usually related to teams with whom they've worked previously. They're expected to perform various security activities throughout an application's development cycle.

Security Champions undergo specific training to build new skills needed to perform activities at different stages of the SDLC. In this capacity, Security Champions oversee adherence to the organization's secure SDLC.

Merits of the activity-focused approach:

- Provides a way to scale security activities throughout the organization's development teams
- Nurtures the organic growth and development of new security experts
- Assigns dedicated security experts to applications

An activity-focused program might require the Champion to perform the following tasks during the SDLC:

Requirements	Design	Implementation	QA	Production
Security requirements review	Threat modeling	SAST onboarding Remediation guidance	DAST onboarding Remediation guidance	Incident response support

Example set of responsibilities for a Security Champion in an activity-focused program

While activity-focused programs provide a great deal of value, they're more complicated to establish. They involve careful attention and maintenance. And they require a greater time commitment, which can also seem costly—though if they are created and managed effectively, the benefits will greatly outweigh the costs.

Hybrid programs

Funding full-time Security Champions isn't realistic for most organizations. Instead, many have put together successful hybrid approaches that find a middle ground between training-focused and activity-focused programs. In hybrid programs, part-time Security Champions are responsible for providing remediation guidance and performing a smaller set of security activities while maintaining their responsibilities as developers. Thus, the SSG can still provide value while managing costs

What are the qualities of a successful Security Champions program?

Community. Successful Security Champions programs build a community with which Champions can engage. This can include a forum to discuss questions, help one another with security activities, and explore changing industry trends. Additionally, program administrators can schedule periodic technical security talks with external speakers. It's important to provide an avenue to nurture Champions' learning.

Growth. When new Security Champions join the program, they're often unfamiliar with software security practices. Consequently, security training is a critical aspect of any Security Champions program. To promote growth through the program and recognize high achievers, you can structure progress with an achievement recognition system.

For instance, new Champions might start the program as white belts. As they move through the initial training, they can become yellow belts only after they demonstrate a specified level of proficiency. In keeping with this karate belt example, advanced Champions are promoted to black belts once they've become subject matter experts. Or perhaps they can earn this rank for playing a part in the evolution of the Security Champions program.

Leadership. Maintaining a successful Champions program requires attention; therefore, someone must be responsible for program administration. Depending on the program complexity, the administrator can move forward in a part-time or full-time role.

Security Champions administrator responsibilities:

- Tracking the progress of Security Champions
- Soliciting development teams for new Champion nominations
- Managing the community
- Scheduling and coordinating technical talks and outside speakers
- Tracking and reporting metrics
- Evolving the Security Champions program as requirements change

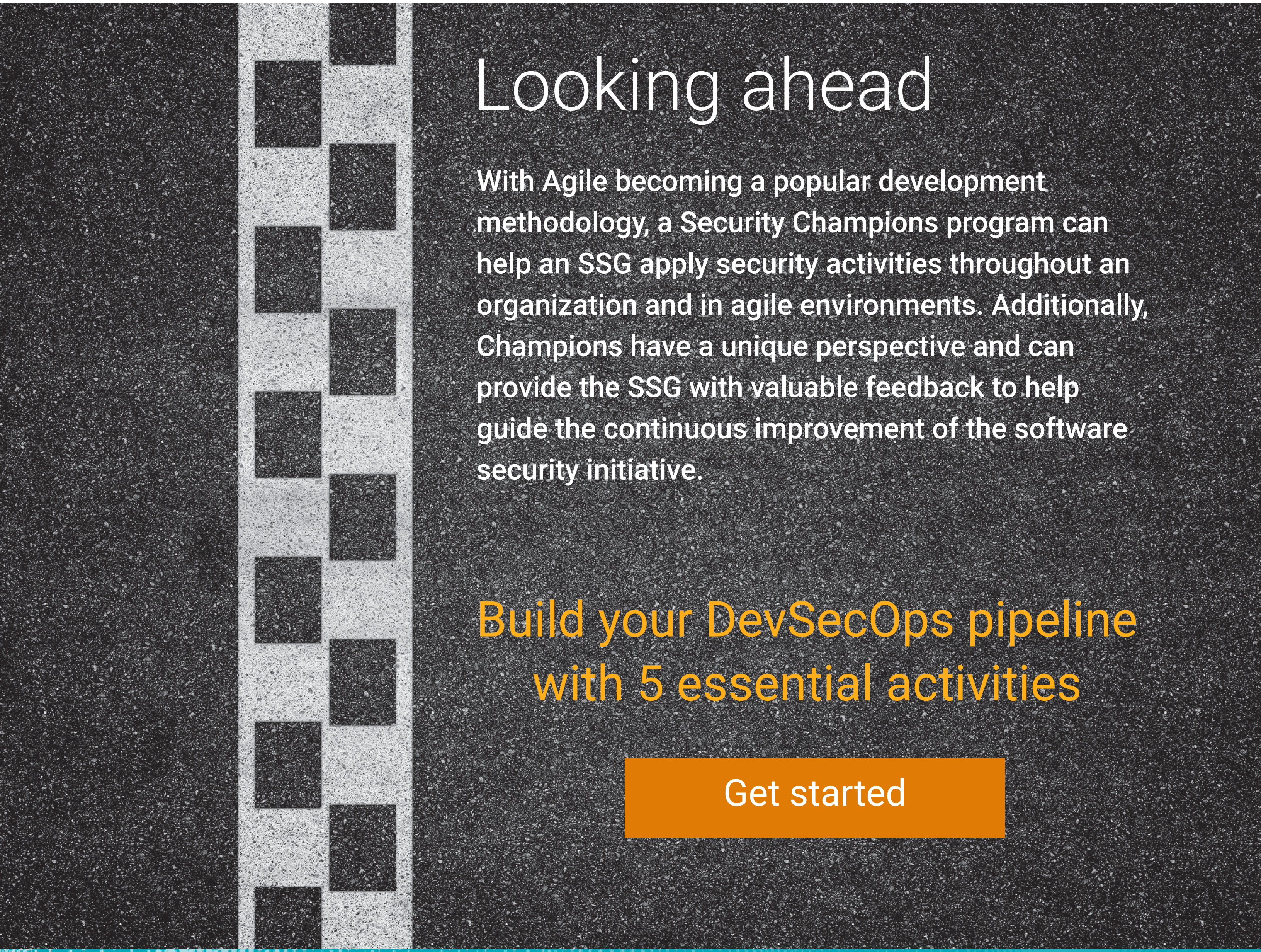
For activity-focused programs, one option is to create a Security Champions coach role. Coaches are responsible for mentoring Champions and aiding them in learning new security activities. In addition, coaching can be a way for more advanced Champions to give back to the program.

What are the selection criteria for Security Champions?

It’s important to note some qualities that make a good Security Champion. Candidates provide the most value when they can draw on past development experiences. To do this, Champions must have experience working as developers within a company’s development organization. One way to find Champions is to seek nominations from application owners and stakeholders within this organization. The best way is to recruit those developers who are self-starters in software security topics.

Additional Security Champions criteria:

- At least 2 years of software development experience
- Leadership skills or potential
- Strong communication skills
- Hands-on technical proficiency in languages and frameworks within their domain
- Demonstration of application security aptitude through participation in existing application security activities



Looking ahead

With Agile becoming a popular development methodology, a Security Champions program can help an SSG apply security activities throughout an organization and in agile environments. Additionally, Champions have a unique perspective and can provide the SSG with valuable feedback to help guide the continuous improvement of the software security initiative.

Build your DevSecOps pipeline with 5 essential activities

Get started

BLACKDUCK®

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.